FortiClient v5.0 Patch Release 3
Administration Guide

FortiClient v5.0 Patch Release 3 Administration Guide

May 27, 2013

04-503-183401-20130527

Copyright© 2013 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, and FortiGuard®, are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance metrics contained herein were attained in internal lab tests under ideal conditions, and performance may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to the performance metrics herein. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any guarantees. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Technical Documentation	docs.fortinet.com
Knowledge Base	kb.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Table of Contents

Change Log

Date	Change Description
2012-11-02	Initial release.
2012-11-07	Updated scripts chapters. This document is now inclusive of both Windows and Mac OS X. It is important to note that not all features available for Windows are available for Mac OS X.
2012-11-15	Updated IPsec and SSL VPN chapter.
2012-11-22	Added note about FortiClient License for FortiAuthenticator.
2012-11-27	Updated script commands to match changes in the *FortiClient v5.0 XML Reference*.
2013-01-09	Updated for FortiClient v5.0 Patch Release 1. Removed XML chapter, see to the *FortiClient v5.0 XML Reference* for more information. Removed FortiClient Tools chapter, see the *FortiClient v5.0 Patch Release 1 Release Notes* for more information.
2013-04-05	Updated for FortiClient v5.0 Patch Release 2. Added new chapter for SCCM 2012.
2013-04-29	Minor update for FortiClient v5.0 Patch Release 3.
2013-05-27	Fixed typographic error.

Introduction

FortiClient has been completely re-designed for v5.0. FortiClient provides a comprehensive network security solution for endpoints while improving your visibility and control. FortiClient allows you to manage the security of multiple endpoint devices from the FortiGate interface. This document provides an overview of FortiClient v5.0.

This document was written for FortiClient (Windows) v5.0 Patch Release 3. Not all features described in this document are supported for FortiClient (Mac OS X) v5.0 Patch Release 3.

Licensing

Licensing on the FortiGate is based on the number of registered clients. FortiGate 40C series and higher models support ten (10) free managed FortiClient licenses. For additional managed clients, an upgraded license must be purchased. The maximum number of managed clients varies per device model.

Client limits

The following table shows client limits per FortiGate model series:

Table 1: FortiClient license upgrade

FortiGate Series	Free registrations	FortiClient license upgrade SKU
FortiGate/FortiWiFi 40 series	10	No upgrade license.
FortiGate/FortiWiFi 60C, 60D, 80C, 90D series	10	200 client registrations FCC-C0102-LIC
FortiGate 100, 200, 300, 600, 800 series, VM01/VM01-XEN, VM02/VM02-XEN	10	2000 client registrations FCC-C0103-LIC
FortiGate 1000, 3000, 5000 series, VM04/VM04-XEN, VM08/VM08-XEN	10	8000 client registrations FCC-C0105-LIC

In high availability (HA) configurations, all cluster members require an upgrade license key.

For more information, go to www.forticlient.com.

Supported operating systems

FortiClient v5.0 Patch Release 3 supports the following operating systems:

Microsoft Windows

- Microsoft Windows 8 (32-bit and 64-bit)
- Microsoft Windows 7 (32-bit and 64-bit)
- Microsoft Windows Vista (32-bit and 64-bit)
- Microsoft Windows XP (32-bit)

Mac OS X

- Mac OS X v10.8 Mountain Lion
- Mac OS X v10.7 Lion
- Mac OS X v10.6 Snow Leopard

Minimum system requirements

FortiClient v5.0 Patch Release 3 requires the following for installation:

Microsoft Windows

- Microsoft Internet Explorer 8.0 or later
- Windows compatible computer with Pentium processor or equivalent
- Compatible operating system and minimum RAM: 512MB
- 600 MB free hard disk space
- Native Microsoft TCP/IP communication protocol
- Native Microsoft PPP dialer for dial-up connections
- Ethernet NIC for network connections
- Wireless adapter for wireless network connections
- Adobe Acrobat Reader or another PDF reader for user manual
- MSI installer 3.0 or later

Mac OS X

- Intel processor
- 256MB of RAM
- 20MB of hard disk drive (HDD) space
- TCP/IP communication protocol
- Ethernet NIC for network connections
- Wireless adapter for wireless network connections

Language support

The following table lists FortiClient language support information.

Table 2: Language support

Language	Graphical User Interface	XML Configuration	Documentation
English (United States)	✔	✔	✔
French	✔	-	-
German	✔	-	-
Portuguese (Brazil)	✔	-	-
Spanish (Spain)	✔	-	-
Chinese (Simplified)	✔	-	-
Chinese (Traditional)	✔	-	-
Japanese	✔	-	-
Korean	✔	-	-

Please review the *FortiClient v5.0 Patch Release 3 (Windows) Release Notes* or the *FortiClient v5.0 Patch Release 3 (Mac OS X) Release Notes* prior to upgrading. Release Notes are available at the Customer Service & Support site.

FortiClient language is dependent on the regional settings on the client workstation. When the regional language setting is not supported, FortiClient defaults to English. When configuring language in the XML configuration file, the language setting overrides the regional language settings of the client workstation.

What's New in FortiClient v5.0

Summary of enhancements

This document was written for FortiClient (Windows) v5.0 Patch Release 3. Not all features described in this document are supported for FortiClient (Mac OS X) v5.0 Patch Release 3.

The following is a list of enhancements in FortiClient v5.0.

FortiClient (Windows) v5.0 Patch Release 3

- Enhancements to FortiProxy
- Improved VPN usability with FortiToken

FortiClient (Windows) v5.0 Patch Release 2

- Customizable console for registered clients
- Endpoint control registration with redundant gateways

  Enables roaming clients
- Enhancement to the remembered FortiGates feature
- FortiClient uploads traffic, event, and vulnerability scan logs to FortiAnalyzer/FortiManager

  Requires a FortiAnalyzer/FortiManager device running v5.0 Patch Release 3 or later and a FortiGate device running v5.0 Patch Release 3 or later. In this release FortiClient logs are stored only. Support to view logs and create reports based on FortiClient logs will be added in a future release.
- SSL VPN realm support (command line)
- Updated OpenSSL to 1.0.1e
- Synchronize VPN elements; *save password*, *auto connect*, and *always up*; with the FortiGate

  Requires a FortiGate running FortiOS v5.0 Patch Release 3.
- Web category filtering safe search support

  For popular search sites or portals including Google, Bing, Yahoo, and Yandex.

FortiClient (Windows) v5.0 Patch Release 1

- Endpoint Control registration over SSL VPN or IPsec VPN
- Remember multiple FortiGates for Endpoint Control registrations
- FortiClient console improvements

FortiClient (Windows) v5.0.0

- Antivirus and Antimalware

  Protection against the latest virus, grayware (adware/riskware) threats.

  Client antivirus is free, and auto updates every three hours.
- Application firewall

  Block, allow, and monitor applications that send traffic to the network.
- Bring Your Own Device (BYOD)

- Diagnostic tool
- Enhancements to the FortiClient console
- Endpoint Management using FortiGate, including:

  Automatic endpoint registration. User initiated endpoint registration.

  Deploy VPN (IPsec/SSL) configuration

  Enable/disable antivirus real-time protection.

  Manage/deploy web filtering and application firewall configuration.
- Localization support
- Parental Control/Web Filter

  Block, allow, warn, and monitor web traffic based on category.
- Remote Access (IPsec and SSL VPN)

  Secure Virtual Private Network access to your network.

  Supports multiple gateways for a single tunnel.
- Rootkit detection and removal
- Single Sign-On Mobility agent support with FortiAuthenticator/FSSO collector agent
- Support automatic executing of a custom batch script via an IPsec VPN tunnel
- Support multiple (maximum 10) gateway IP/FQDN in a single IPsec VPN configuration
- Support XML configuration
- VPN from system tray
- VPN auto connect/always up

  Support ability to automatically connect to a VPN tunnel without user interaction

  Support ability to configure the VPN to always be connected
- Vulnerability scan

  Identify system and application vulnerabilities.

FortiClient (Mac OS X) v5.0 Patch Release 3

- Improved VPN usability with FortiToken

FortiClient (Mac OS X) v5.0 Patch Release 2

- Customizable console for registered clients
- Endpoint control registration with redundant gateways (maximum 20)

  Enables roaming clients.
- Enhancements to the remembered FortiGates feature
- FortiClient uploads traffic and vulnerability scan logs to FortiAnalyzer/FortiManager

  Requires a FortiAnalyzer/FortiManager device running v5.0 Patch Release 3 or later and a FortiGate device running v5.0 Patch Release 3 or later.
- FortiClient console improvements
- FortiClient traffic logging
- Improved VPN controller reliability
- Silent registration element added to the `endpoint_control` section in the XML configuration file.
- Synchronize VPN elements; `save password`, `auto connect`, and `always up`; with the FortiGate. Requires a FortiGate running FortiOS v5.0 Patch Release 3.
- Web category filtering safe search support

  For popular search sites or portals including: Google, Bing, Yahoo, and Yandex.

FortiClient (Mac OS X) v5.0 Patch Release 1

- Remember multiple FortiGates for Endpoint Control registrations
- Endpoint Control registration over SSL VPN and IPsec VPN
- Improvements to the FortiClient GUI
- Splash screen
- VPN resiliency

FortiClient (Mac OS X) v5.0.0

- AntiVirus and Antimalware
  Protection against the latest virus, grayware (adware/riskware) threats.
  Client antivirus is free, and auto updates every three hours.
- Application Firewall
  Block, allow, and monitor applications that send traffic to the network.
- Bring Your Own Device (BYOD)
- Diagnostic Tool
- Enhancements to the FortiClient dashboard
- Endpoint Management using FortiGate, including:
  Automatic endpoint registration. User initiated endpoint registration.
  Deploy VPN (IPsec/SSL) configuration
  Enable/disable AntiVirus real-time protection.
  Manage/deploy Web Filtering and Application Firewall configuration.
- Localization support
- Parental Control/Web Filter
  Block, allow, warn, and monitor web traffic based on category.
- Remote Access (IPsec and SSL VPN)
  Secure Virtual Private Network access to your network.
  Supports multiple gateways for a single tunnel.
- Single Sign-On Mobility Agent support with FortiAuthenticator/FSSO Collector Agent
- Support automatic executing of a custom batch script via an IPsec VPN tunnel
- Support multiple (maximum 10) gateway IP/FQDN in a single IPsec VPN configuration
- Support XML configuration
- VPN from system tray
- VPN auto connect/always up
  Support ability to automatically connect to a VPN tunnel without user interaction
  Support ability to configure the VPN to always be connected
- Vulnerability Scan
- Identify system and application vulnerabilities.

Download and Install FortiClient

Download FortiClient

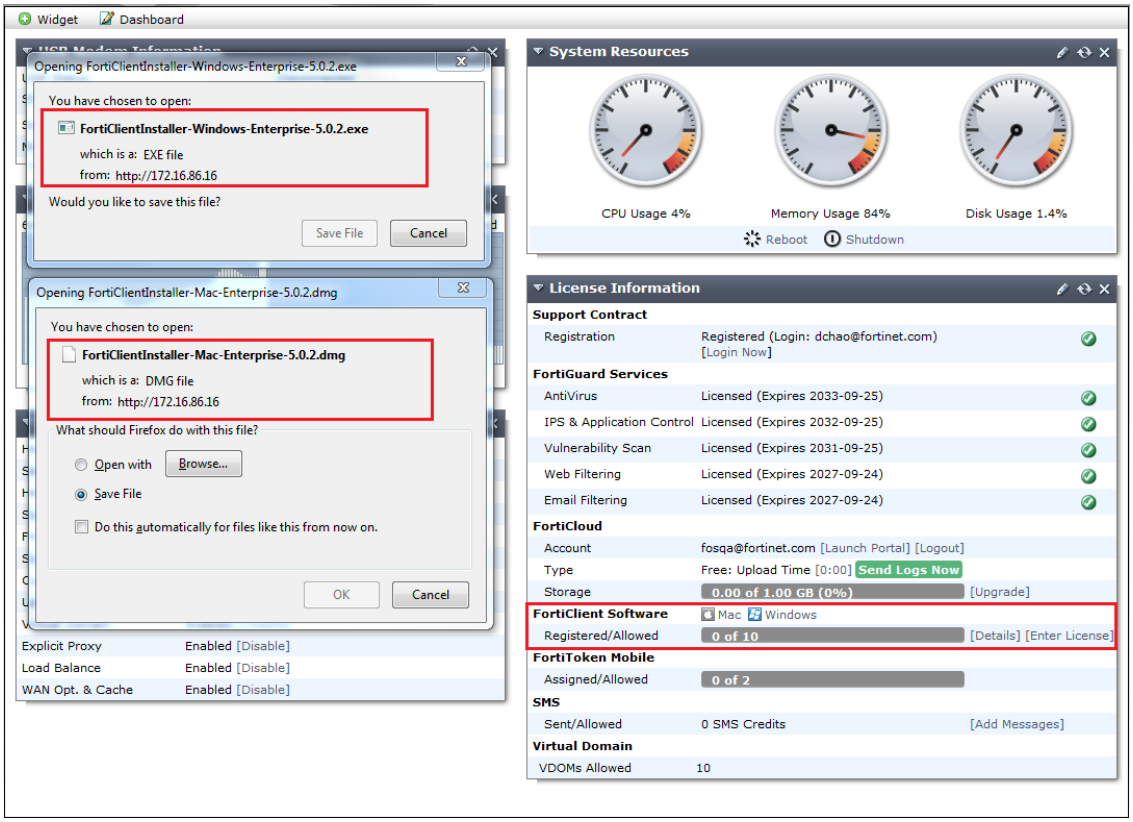
The installation file can be downloaded from the following sites:

- Fortinet Customer Service & Support: https://support.fortinet.com

  Requires a support account with a valid support contract. The installation file is available for both 32-bit and 64-bit systems for Microsoft Windows.
- FortiClient homepage: www.forticlient.com

In FortiOS v5.0 Patch Release 1 or later, you can download the FortiClient installation files in the FortiOS dashboard. Go to *System* > *Dashboard* > *Status,* in the *License Information* widget, select *Mac* or *Windows* to download the FortiClient installation files.

Figure 1: License information widget



Install FortiClient on a Microsoft Windows computer

The following instructions will guide you though the installation of FortiClient on a Microsoft Windows computer. For more information, see the *FortiClient (Windows) v5.0 Patch Release 3 Release Notes*.

To install FortiClient (Windows):

1. Double-click the FortiClient executable file to launch the setup wizard. The *Setup Wizard* will install FortiClient on your computer.

   The *Welcome* screen appears.

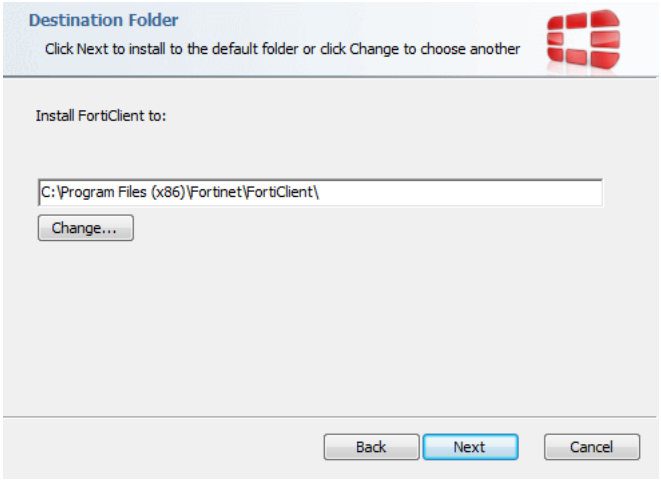
   Figure 2: Welcome screen

2. Read the license agreement and select *Next* to continue. You have the option to print the EULA in this window.

   Figure 3: End-User License Agreement page

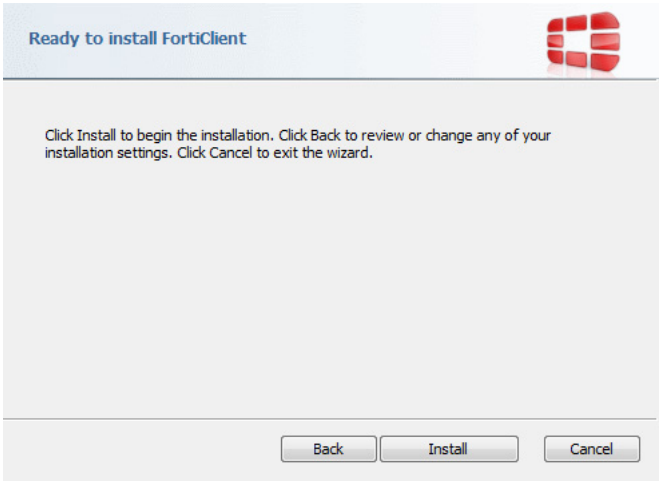
3. Select *Change* to choose an alternate folder destination for installation. Select *Next* to continue.

Figure 4: Destination folder selection page



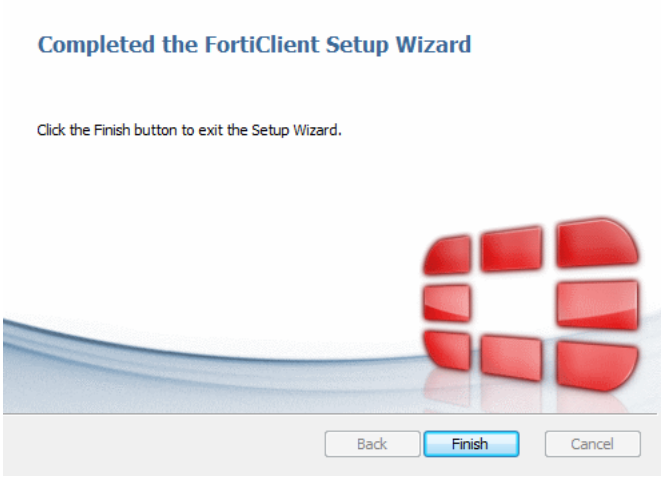
4. Select *Install* to continue.

Figure 5: Ready to install FortiClient page



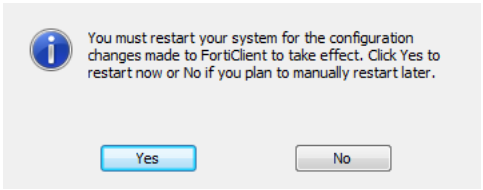
5. Select *Finish* to exit the FortiClient Setup Wizard.

Figure 6: Installation completed page



6. On a new FortiClient installation, you do not need to reboot your system. When upgrading the FortiClient version, you must restart your system for the configuration changes made to FortiClient to take effect. Select *Yes* to restart your system now, or select *No* to manually restart later.

Figure 7: System restart confirmation dialog box



7. To launch FortiClient, double-click the desktop shortcut icon.

Figure 8: FortiClient desktop shortcut

Install FortiClient on a Mac OS X computer

The following instructions will guide you though the installation of FortiClient on a Mac OS X computer. For more information, see the *FortiClient (Mac OS X) v5.0 Patch Release 3 Release Notes.*

To install FortiClient (Mac OS X):

1. Double-click the FortiClient .dmg installer file to launch the FortiClient installer. The *FortiClient Installer* will install FortiClient on your computer. Select *Continue*.

Figure 9: Welcome screen

2. Read the Software License Agreement and select *Continue*. You have the option to print or save the Software Agreement in this window. You will be prompted to *Agree* with the terms of the license agreement.

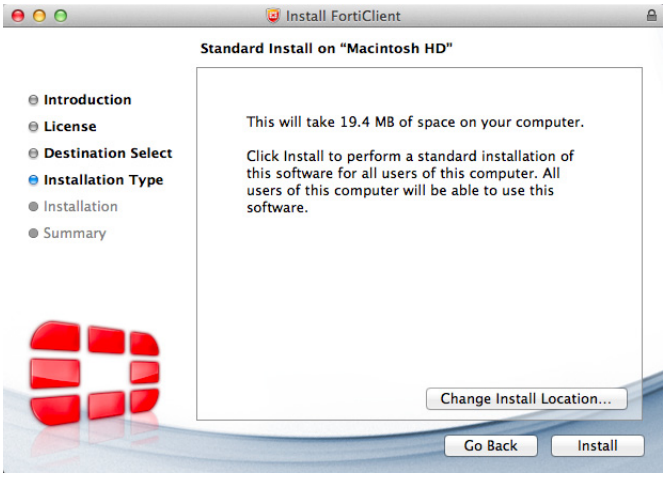
Figure 10: Software License Agreement page

3. Select the destination folder for the installation.

Figure 11: Destination select page

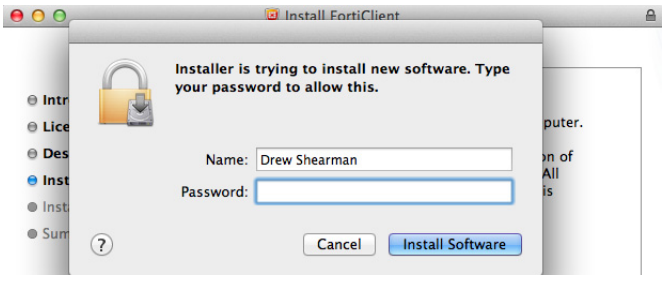
4. Select *Install* to perform a standard installation on this computer. You can change the install location from this screen.

Figure 12: Installation type page



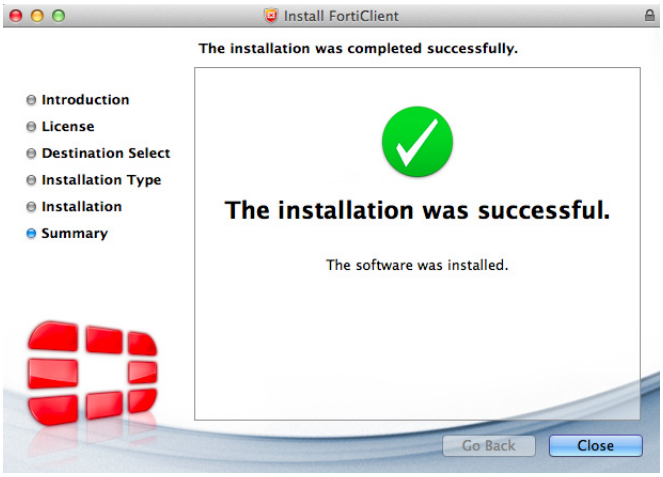
5. Depending on your system, you may be prompted to enter your system password.

Figure 13: Enter system password to continue



6. The installation was successful. Select *Close* to exit the installer.

Figure 14: The installation was successful

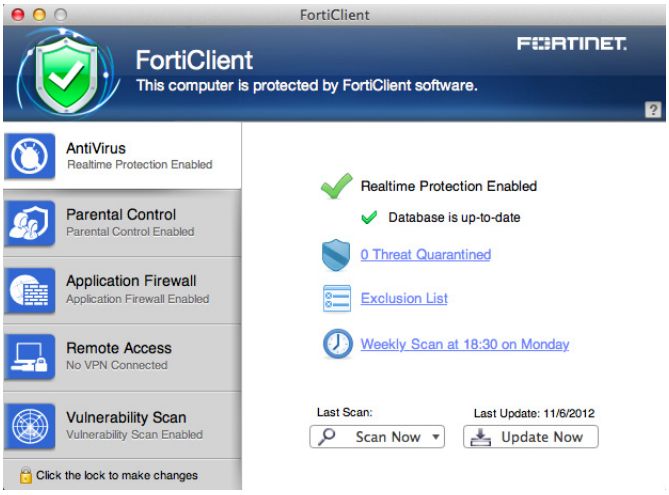


7. FortiClient has been saved to the Applications folder.

Figure 15: Applications folder

8. Double-click the FortiClient icon to launch the application. The application console loads to your desktop. Select the lock icon in the FortiClient console to make changes to the FortiClient configuration.

Figure 16: Default FortiClient console is locked



Provisioning FortiClient

FortiClient MSI configuration tool

The *FortiClient Configurator* tool is the recommended method of creating a customized installation of FortiClient.

This document was written for FortiClient (Windows) v5.0 Patch Release 3. Not all features described in this document are supported for FortiClient (Mac OS X) v5.0 Patch Release 3.

Usage

```
FortiClientConfigurator.exe -m <path to FortiClient.msi file>
     [optional switches]
```

Switches and switch parameters are case sensitive.

Use the following switch to prevent users from changing FortiClient settings:

```
-m <path to FortiClient msi file> (Required)
--REGISTRATIONKEY <key>
```

FortiClient will attempt to register to this FortiGate. If it cannot, it will try to register to the default gateway. When its details are discovered, the FortiGate default gateway will appear in the FortiClient console and the user can register to it.

```
--FGTIP <ip:port or fqdn:port>
```

Use the following switch to specify a list of FortiGates that FortiClient should register with:

```
--REDUNDANTFGTIPS <ip:port or fqdn:port>[,<ip:port or fqdn:port>]...
```

When the following switch is specified, FortiClient will not prompt users to confirm registration to FortiGates. Registration is only silent for FortiGates specified by `--REDUNDANTFGTIPS`.

```
--SILENTREGISTRATION
```

Example usage

```
FortiClientConfigurator.exe -m c:\downloads\forticlient.msi
     --REGISTRATIONKEY sercretpassword
```

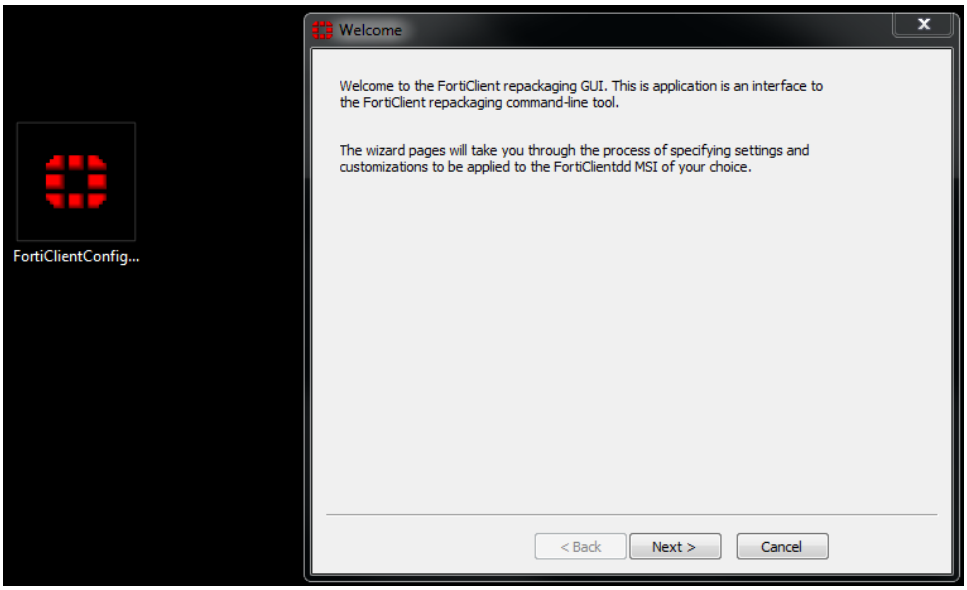
This command above creates the following directories containing files ready for deployment:

```
c:\downloads\FortiClient_packaged\ActiveDirectory\
c:\downloads\FortiClient_packaged\ManualDistribution\
```

FortiClient Configurator application

The FortiClientConfiguratorGUI tool is an application interface to the FortiClient repacking command line tool. The wizard will guide you through the process of specifying settings to be applied to the FortiClient MSI file.

Figure 17: FortiClient Configuration application interface



Creating a custom MSI installation file

You can create a custom MSI installer file for your customized FortiClient Application:

1. Determine the command line options you need for your customized FortiClient installer.
2. In the folder where you expanded the installer .zip package, execute the following command line entry:

   ```
   FortiClientConfigurator.exe -m <path to FortiClient.msi file>
       <optional switches>
   ```

   A new subdirectory is created, which contains the FortiClient MSI file.

For more information on FortiClient XML configuration, see the *FortiClient v5.0 Patch Release 3 XML Reference* at the Fortinet Technical documentation site, http://docs.fortinet.com.

Deploy FortiClient using Microsoft Active Directory (AD) server

There are multiple ways to deploy FortiClient to endpoint devices using Microsoft Active Directory.

The following instructions are based from Microsoft Windows Server 2008. If you are using a different version of Microsoft Server, your MMC or snap-in locations may be different.

Using Microsoft AD to deploy FortiClient:

1. On your domain controller, create a distribution point.
2. Log on to the server computer as an administrator.
3. Create a shared network folder where the FortiClient MSI installer file will be distributed from.
4. Set file permissions on the share to allow access to the distribution package. Copy the FortiClient MSI installer package into this share folder.
5. Select *Start* > *Administrative Tools* > *Active Directory Users and Computers*.
6. After selecting your domain, right-click to select a new Organizational Unit (OU).
7. Move all the computers you wish to distribute the FortiClient software to into the newly-created OU.
8. Select *Start* > *Administrative Tools* > *Group Policy Managemen*t. The Group Policy Management MMC Snap-in will open. Select the OU you just created. Right-click it, *Select Create a GPO* in this domain, and Link it here. Give the new GPO a name then select OK.
9. Expand the Group Policy Object container and find the GPO you just created. Right-click the GPO and select Edit. The Group Policy Management Editor MMC Snap-in will open.
10. Expand *Computer Configuration* > *Policies* > *Software Settings*. Right-click Software Settings and select *New* > *Package*.
11. Select the path of your distribution point and FortiClient installer file and then select *Open*. Select *Assigned* and select *OK*. The package will then be generated.
12. If you wish to expedite the installation process, on both the server and client computers, force a GPO update.
13. The software will be installed on the client computer's next reboot. You can also wait for the client computer to poll the domain controller for GPO changes and install the software then.

Uninstall FortiClient using Microsoft Active Directory server:

1. On your domain controller, select *Start* > *Administrative Tools* > *Group Policy Management*. The Group Policy Management MMC Snap-in will open. Expand the Group Policy Objects container and right-click the Group Policy Object you created to install FortiClient and select Edit. The Group Policy Management Editor will open.
2. Select *Computer Configuration* > *Policy* > *Software Settings* > *Software Installation*. You will now be able to see the package that was used to install FortiClient.
3. Right-click the package, select *All Tasks* > *Remove*. Choose Immediately uninstall the software from users and computers, or *Allow* users to continue to use the software but prevent new installations. Select *OK*. The package will delete.
4. If you wish to expedite the uninstallation process, on both the server and client computers, force a GPO update as shown in the previous section. The software will be uninstalled on the client computer's next reboot. You can also wait for the client computer to poll the domain controller for GPO changes and uninstall the software then.

System Center Configuration Manager

Introduction

These instructions assume you have already installed and configured SCCM. If you have not, please refer to Microsoft's online help sources for information on this task.

The Microsoft *System Center 2012 Configuration Manager* (SCCM) may be used to deploy and manage multiple FortiClient Installations. This chapter presents various scenarios that you can utilize.

A fully functional SCCM server, along with discovered devices, is required. Visit the Microsoft web site for supporting documentation.

The following topics are detailed in this section:

- SCCM setup
- Task sequences
- Task sequence examples for FortiClient.

SCCM setup

Microsoft maintains a public free virtual lab of the *System Center 2012 Configuration Manager* (SCCM) at http://technet.microsoft.com/virtuallabs/bb539977.

At this page you can access a completely installed and properly configured system that can be used for testing various SCCM deployment scenarios. For ongoing enterprise use, a new system has to be created and configured.

SCCM product home page: http://www.microsoft.com/server-cloud/system-center

Technet documentation: http://technet.microsoft.com/systemcenter

Microsoft documentation: http://www.microsoft.com/en-ca/download/details.aspx?id=29901

The following subsections discuss some of the preparations required to enable control of FortiClient host computers.

Client discovery options and configuration

The *Configuration Manager* uses various methods to discover the Windows devices that an administrator can control on the network. One such method is the use of a common domain. To use this method, the Windows server hosting the *Configuration Manager* should be configured as domain controller. All Windows devices that will be managed should then join the domain. The *Configuration Manager* automatically discovers all Windows devices that join.

Installation of clients

The *Configuration Manager* console may be used to install configuration manager client software on target Windows devices that have joined the controlled domain. This is required for pushing the configuration to the devices.

Client policy polling interval settings

The configuration manager client on each Windows device polls for policy changes on the server at a regular interval. The polling interval defaults to 60 minutes. Each newly pushed or deployed task will run on all selected clients within this polling interval. You can customize the polling interval as required.

Client collections

New configurations are usually deployed to collections of devices. All of the devices that have joined the controlled domain will be added to a default collection.

You may want to deploy a different set of configurations to different groups of devices based on your user base. This can be accomplished by creating different client collections. Devices that have joined the domain will be added to one or more of those collections. Configurations may then be selectively deployed.

Client security issues

The *Configuration Manager* is able to deploy a large variety of applications to all the devices that joined the domain. Most of these tasks run with the administrator or system user authorisation level on the client devices. It is important to keep the *Configuration Manager* host under the highest level of security control possible.

It is also important to always test new planned application deployments in a controlled lab environment, or on a small client collection, before deploying to the entire client base.

Network share for all clients

The *Configuration Manager* console is used to deploy applications to client devices. Some of the applications require specification of files by file path and name. The client devices must have access to the files when the applications run. For instance, to upload a FortiClient XML configuration file to a given client collection, all client devices in the collection must independently have local access to the new XML configuration file.

The files may be provided by any suitable method. Examples include use of an HTTP or FTP server. The examples in this document use a network share. This should be available to all devices on the given client collection.

Task sequences

The *Configuration Manager* provides task sequences as a means of deploying commands to discovered clients without requiring user intervention. The FortiClient configuration examples in this chapter use the *Run Command Line* task sequences to run various command-line commands on client devices.

Task sequences are described in the following Microsoft documents:

Planning a Task Sequence Strategy

http://technet.microsoft.com/en-us/library/gg712685.aspx

How to Manage Task Sequences

http://technet.microsoft.com/en-us/library/hh273490.aspx

Here is a simple example of how task sequences may be used to control client devices.

In this example, a simple set of command-line commands are created in the *Configuration Manager* console. Once deployed, the commands will print information requested to the log file for each client.

The following commands will be executed on each client:

```
cd
dir c:\users
whoami
```

The first command will print the current working directory. This is likely to be `c:\windows\system32`. The second command will print the contents of the specified directory. The third command will print the name of the current user (the user under which the task sequence is running).

The output of the commands can be found in the log file on each client device at:

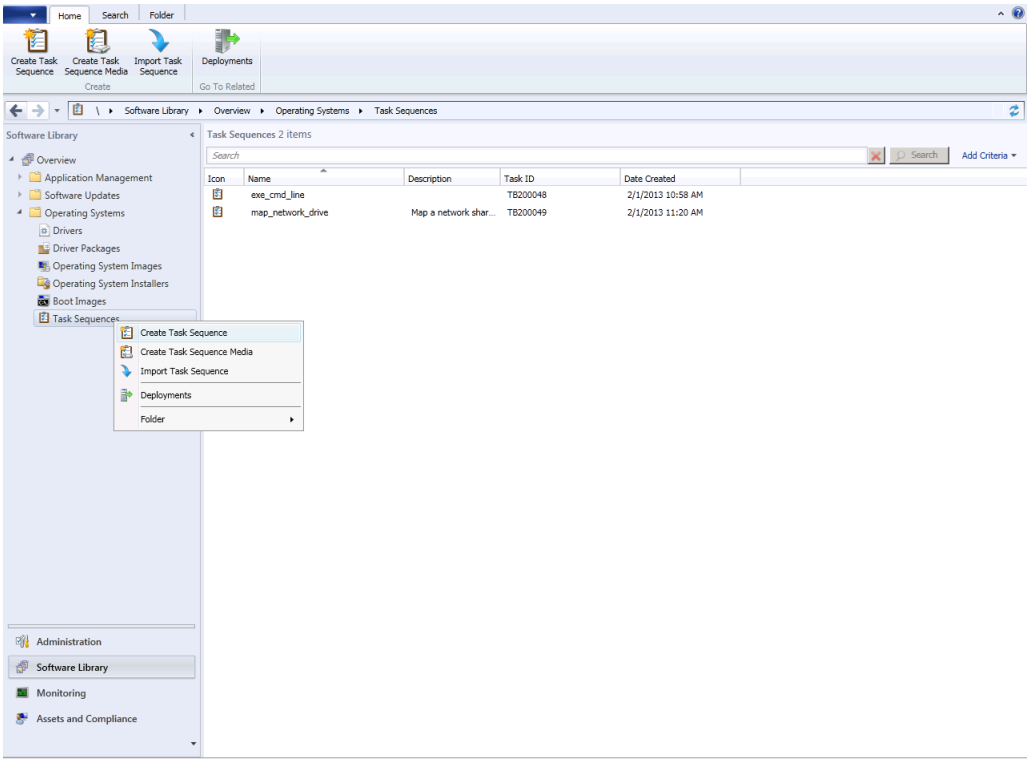
```
C:\Windows\CCM\Logs\smsts.log
```

To create a new task sequence:

1. Launch the *Configuration Manager* console.

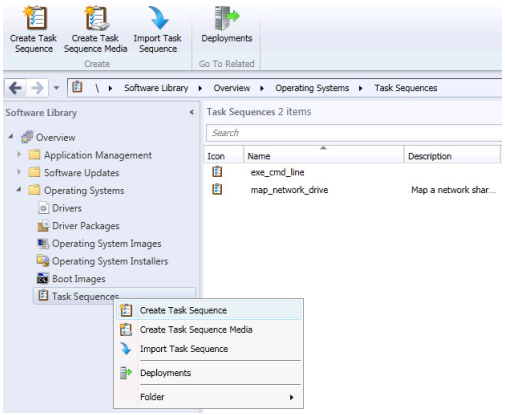
   The *Configuration Manager* console appears.

Figure 18:SCCM configuration manager



2. Select *Software Library* > *Overview* > *Operating Systems* > *Task Sequences.*
3. Right-click the *Task Sequence* menu item and select *Create Task Sequence.*

Figure 19: Right-click menu

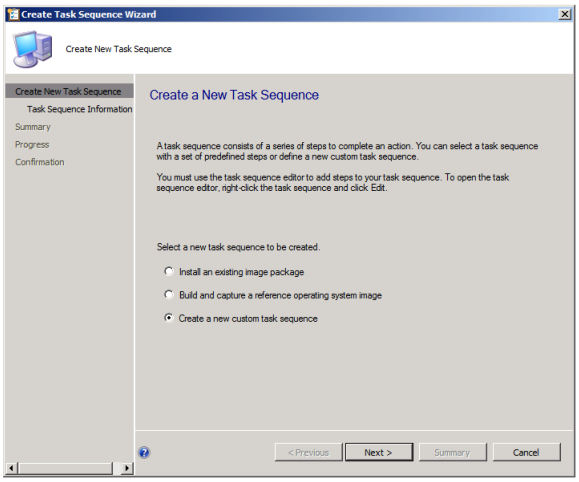


Alternatively, you can select *Create Task Sequence* in the toolbar.

Figure 20: Toolbar menu items

The *Create Task Sequence Wizard* opens.

Figure 21: Create task sequence task wizard



4. Select the *Create a new custom task sequence* radio button. Then select *Next* to proceed.
5. Enter a name for the task sequence.
6. Enter a comment to describe the task sequence.
7. Select *Next* to proceed.

   A summary of the task sequence configuration is displayed.
8. Select *Close* to save the configuration. The new task sequence is created and displayed in the *Configuration Manager* console.
9. Select *Task Sequences* in the menu in the left pane of the *Configuration Manager* console. The new task sequence is displayed in the right pane.

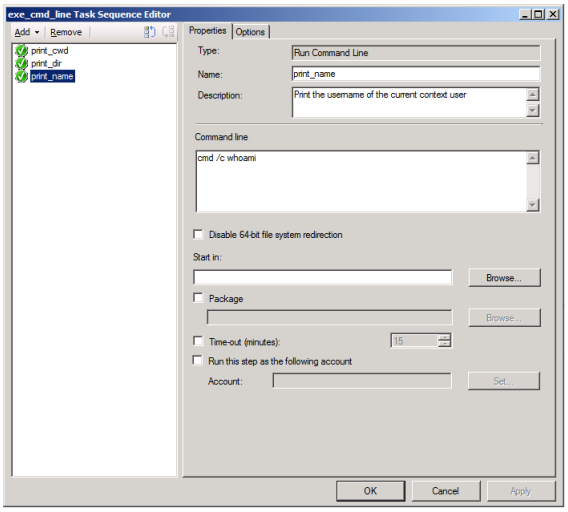
To add individual tasks into the task sequence:

1. Right-click in the newly created task sequence.
2. From the shortcut menu list, select *Edit*. The Task Sequence Editor dialog box is displayed.

   Alternatively, select the *Task Sequence* and select the *Edit* icon in the toolbar.
3. Select the *Add* drop-down button.
4. From the drop-down list, select *General* and the select *Run Command Line.*

   A new tab is displayed in the right pane of the dialog box.

Figure 22: Command line window



5. Configure the following settings:

Name	Enter a name for the command.
Description	Enter a description for the command.

Command line	Enter the command line in the text field.
	The command will usually start with “cmd /c”. For instance, the first command in this example is entered as:
	`cmd /c cd`
	`cmd /c dir c:\users`
	`cmd /c whoami`

6. Select *Apply* to apply the configuration.
7. Select OK to continue.

The task sequence will be saved with the three command-line tasks. To view or modify the tasks, select *Edit* in the short-cut menu for the selected task sequence.

There are three commands in this example. Each of the commands may be created as a single task. There will be a total of three tasks in the left pane of the dialog box. Each of the tasks will have one of the command-line commands:

```
cmd /c cd
cmd /c dir c:\users
cmd /c whoami
```

This format is preferred as it isolates any client errors to a specific task.

The three commands may also be combined into a lengthy single command:

```
cmd /c cd  ;  dir c:\users  ;  whoami
```

This format may mask task sequence errors. It is not recommended.

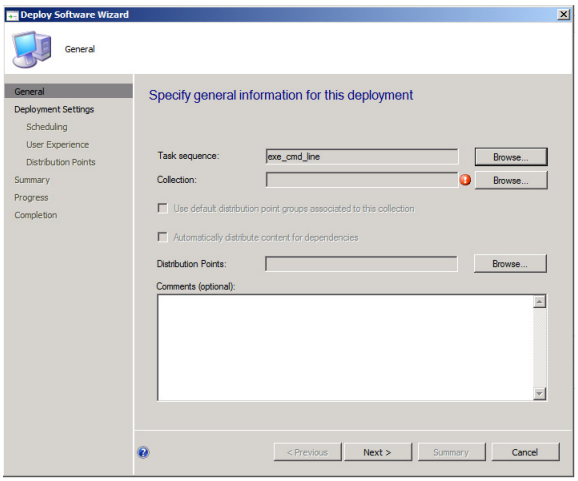
There is also an option to use a batch script.

Deploy the task sequence:

1. Right-click the task sequence.
2. Select *Deploy* in the right-click menu list.

   The *Deploy Software Wizard* dialog box appears.

   Figure 23: Deploy software wizard dialog box

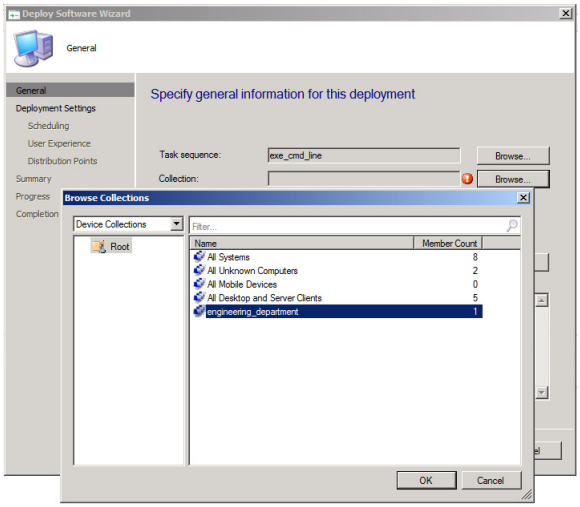


   Alternatively, select the *Task Sequence* and select the *Deploy* icon in the toolbar.

3. Select *Browse*.

   A *Browse Collections* dialog box appears listing all currently configured client collections.

   Figure 24: Browse collections dialog box



4. Select the client collection to which this task sequence should be deployed
5. Select *OK* to close the *Browse Collections* dialog box. Pressing CTRL returns you to the *General* tab of the *Deploy Software Wizard* dialog box.
6. Select *Next*. The *Deployment Settings* tab is displayed
7. In the *Purpose* drop-down menu select *Required*. This makes the task mandatory for all clients receiving it.
8. Select the *Send wake-up packets* checkbox to enable this feature.
9. Select *Next*. The *Scheduling* tab is displayed

10. Select *New*. In the *Assignment Schedule* dialog box select the *Assign immediately after this event* radio button.
11. Select *OK*. This closes the *Assignment Schedule* dialog box. The *Scheduling* tab is displayed.
12. Select *Next*. The *User Experience* tab is displayed.
13. Select the *Show Task Sequence progress* checkbox to enable this feature.

    This configuration is optional. It displays a progress dialog box on each client as the task executes. If a silent background execution of tasks is desired, leave this checkbox unchecked.
14. Select *Next*. The *Distribution Points* tab is displayed. For this example, there is nothing to change in this tab.
15. Select *Next*. The *Summary* tab is displayed.
16. Select *Next*. The *Completion* tab is displayed which shows a summary of all selections.
17. Select *Close* to close the *Deploy Software Wizard*.

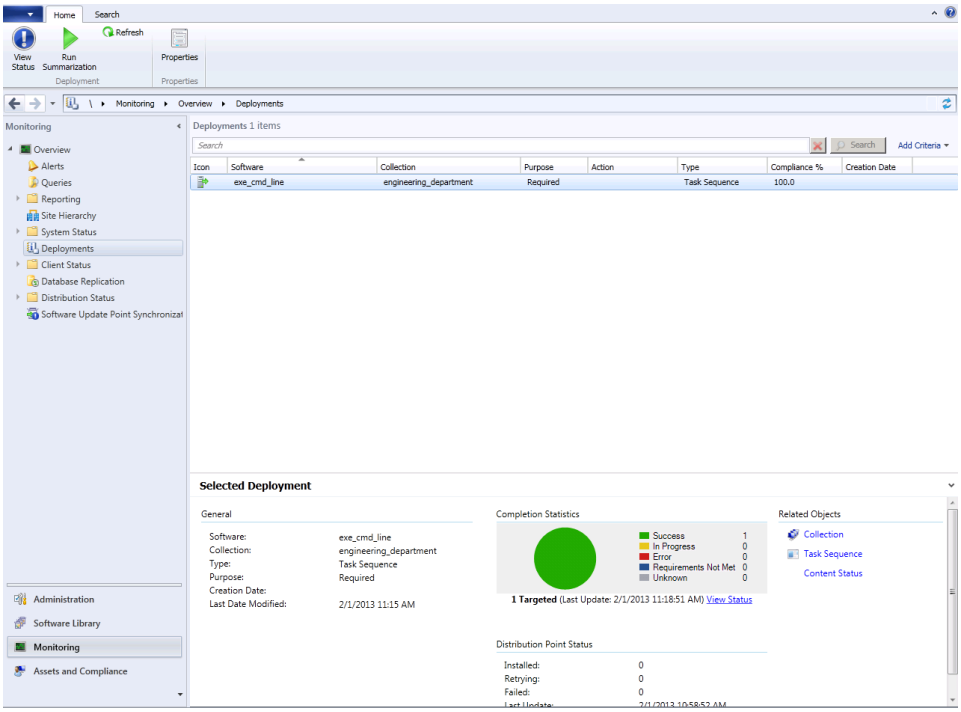
This completes the deployment of the task sequence to the selected client collections. Client devices in the collection should start to receive and execute the task. All clients will run the task within the *Policy Polling Interval* configured.

Monitor a deployed task sequence:

1. Launch the *Configuration Manager* console.
2. Select *Monitoring* from the tree-menu.
3. Select the *Overview* menu item in the left pane to expand the menu.
4. Select the *Deployments* menu item. The list of deployments is displayed in the right pane.
5. Click to select the recently deployed task sequence in the right pane.

   The *Deployments* window is displayed.

Figure 25:.Deployment window



To monitor a deployed task sequence on the client device, use the following process:

1. Launch the *Software Center* console on the client device. It displays a list of tasks deployed to it.

If a recently deployed task sequence is not displayed, most likely the *Policy Polling Interval* is yet to expire on this client.

2. Select the *Task Sequence*. The current status is displayed.

In addition to the two monitoring procedures above, the client log file is available on the client device at:

```
C:\Windows\CCM\Logs\smsts.log
```

It will contain details of the task sequence, including:

- the command-line commands executed
- any output generated by the commands
- any error messages

Mapping a network drive

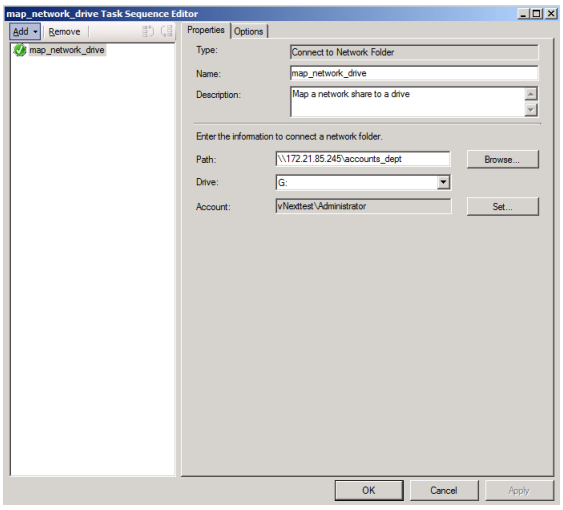
When a file is referenced in a task sequence, it must be made available to all clients before the task sequence starts. The processes listed below explain how to map a network folder to a drive in a given task sequence. If the mapping is successful, all the files in the shared folder will be available for the command-line commands in the Task Sequence.

To map a network drive in the task sequence:

1. Create a new custom task sequence.
2. Edit the task sequence.

   The *Task Sequence Editor* dialog box is displayed.

Figure 26: Task sequence editor dialog box



3. Select the *Add* drop-down button.
4. In the drop-down list, select *General* > *Connect to Network Folder*. A new tab is displayed in the right pane of the dialog box.

5. Type a name for the command.
6. Type a description for the command.
7. Type the full path to the network shared folder or use the *Browse* button to select it.

When using the *Browse* button, be sure that the network share is being reported with the same path as the client devices will use.

Here is an example of a valid path: \\172.21.85.245\accounts_dept

8. Type a drive letter, along with a colon.

   For example: G:
9. Select *Set* and provide a user name and password that is valid for the network shared folder selected.
10. Select *OK* to return to the *Task Sequence Editor* dialog box.
11. Select *Apply* to save the task.

More tasks may be added to the task sequence as described in earlier parts of this section. Tasks may be re-ordered using the other buttons provided in the top of the left pane in the *Task Sequence Editor* dialog box.

When all tasks have been added, select *OK* to close the dialog box.

Task sequence examples for FortiClient

The task sequence processes described in the preceding section may be applied to any regular Windows tasks that runs on the command line. This section discusses several example FortiClient configurations that could be completed from the Windows command-line.

The examples in this section list only the command-line commands to be used. When deploying these from the *Configuration Manager* console, remember to always use the processes discussed this chapter to create the task sequence. The procedure is the same, only the contents of the *Run Command Line* commands will differ.

Install FortiClient

FortiClient can be installed from the command line using `msiexec`. In this example, a FortiClient MSI file that is provided on a network shared folder is used to install FortiClient to devices in the client collection.

Use the following commands in a task sequence to install FortiClient on a Windows client device.

1. Connect to a network folder:
   - Name: `map_network_drive`
   - Description: Mount a network shared directory that contains the FortiClient image to install
   - Path: \\172.21.85.245\accounts_dept
   - Drive: G:
   - Account: `vNexttest\administrator`

2. Run Command Line:
   - Name: `copy_fct_image`
   - Description: Copy FortiClient MSI image from network shared directory
   - Command line: `cmd /c copy /y G:\FortiClient.msi c:\temp\FortiClient.msi`
3. Run Command Line:
   - Name: `install_fct`
   - Description: Install FortiClient using MSI image
   - Command line: `cmd /c msiexec /i c:\temp\FortiClient.msi /qn`

Ensure that the FortiClient.msi file is available in the network share, and that the network share is accessible to all client devices in the client collection before deploying this task sequence.

Export the FortiClient XML configuration file

FortiClient features may be controlled using an XML configuration file. The configuration file is first exported from FortiClient, modified with a text editor, and re-imported into FortiClient. The XML configuration syntax and usage is documented in the *FortiClient v5.0 Patch Release 3 XML Reference*.

Use the following commands in a task sequence to export the XML configuration file from a Windows client device which has FortiClient installed.

1. Connect to a Network Folder:
   - Name: map_network_share
   - Description: Mount a network shared directory to which configuration file will be copied.
   - Path: \\172.21.85.245\engineering_dept
   - Drive: M:
   - Account: vNexttest\administrator
2. Run Command Line:
   - Name: export_fct_xml
   - Description: Export the FortiClient XML configuration file
   - Command line: cmd /c C:\Program Files\Fortinet\FortiClient\fcconfig -o export -f c:\temp\fct_xml.conf
3. Run Command Line:
   - Name: copy_fct_xml
   - Description: Copy FortiClient XML file to network shared directory
   - Command line: cmd /c copy /y c:\temp\fct_xml.conf M:\

This copies fct_xml.conf to the mounted share. If there is more than one device in the client collection, they will each overwrite the same file. You may use a batch script to uniquely rename the file as it is copied.

The full path to the FortiClient installation directory is used as a prefix to FCConfig.exe. The value provided in this example is the default on a 32-bit system. The default on 64-bit systems is:

```
C:\Program Files (x86)\Fortinet\FortiClient
```

If the client collection has a mixture of both 32-bit and 64-bit devices, a batch script may be used to selectively run from the correct platform-dependent directory.

Import a modified XML configuration file

Use the following commands in a Task Sequence to import an XML configuration file into FortiClient in a Windows client device.

1. Connect to a Network Folder:

   Name: map_network_share

   Description: Mount a network shared directory that contains the XML configuration file

   Path: \\172.21.85.245\engineering_dept

   Drive: M:

   Account: vNexttest\administrator

2. Run Command Line:

   Name: copy_fct_xml

   Description: Copy FortiClient XML configuration file from network shared directory

   Command line: cmd / c copy /y M:\fct_xml.conf c:\temp\

3. Run Command Line:

   Name: import_fct_xml

   Description: Import the FortiClient XML configuration file

   Command line: cmd /c “C:\Program Files\Fortinet\FortiClient\fcconfig -o import -f c:\temp\fct_xml.conf”

The same configuration file is used by all devices in the client collection.

Upgrade FortiClient

The FortiClient upgrade process is similar to the regular installation. The only difference is the use of a different version of FortiClient during the installation. A reboot is required, but the task sequence should handle this properly.

The same procedure listed earlier for FortiClient installation could be reused.

Uninstall FortiClient

Use the following command in a task sequence to uninstall FortiClient from Windows client devices.

1. Run Command Line:
   - Name: uninstall_fct
   - Description: Uninstall FortiClient
   - Command line: wmic product where name="FortiClient" call uninstall /nointeractive

The Task Sequence should process the required reboot correctly.

Endpoint Management

Introduction

The purpose of this section is to provide basic instructions on how to configure, deploy, and manage FortiClient configurations from your FortiOS device.

Endpoint Management requires FortiClient v5.0.0 or later and a FortiOS device running v5.0.0 or later, or a FortiOS Carrier device running v5.0.0 or later. Certain features are only available on v5.0 Patch Release 2 or later.

Endpoint Management is available on FG-40C model series and higher devices.

Configure endpoint management

In FortiOS v5.0, configuration and management of FortiClient endpoint agents can now be handled by the FortiGate. You can configure your FortiOS device to discover new devices on your network, enforce FortiClient registration, and deploy a pre-configured endpoint profile to connected devices. The endpoint profile can be deployed to devices on your network and over a VPN connection. You can configure multiple endpoint profiles. The endpoint profile consists of the following sections:

- Antivirus Real-time Protection on Client (when installed)
- Application Firewall

  You can select the application firewall profile to associate with the endpoint profile.
- Web Category Filtering

  You can select the web category filtering profile to associate with the endpoint profile. You can also select to disable Web Category Filtering when the client is protected by the FortiGate.
- Endpoint Vulnerability on Client

  You can select to scan daily, weekly or monthly. You can also select to scan the client after registration with your FortiOS device.
- Client VPN Provisioning

  You can specify the VPN name, type, gateway and other settings the client will use to connect to your FortiOS device via the VPN connection.
- Upload Logs to FortiAnalyzer/FortiManager

  You can select to use the same IP address as the FortiOS device or specify a different device IP address. You can specify the frequency of the log upload.

- Use FortiManager for client software/signature update.

  Select to enable this feature and enter the IP address of your FortiManager device. You can select to failover over to the FortiGuard Distribution Network (FDN) when the FortiManager is not available.
- Client UI Options

  Select to show/hide FortiClient modules in the client console. You can also select to hide banners.

See the *FortiOS Handbook 5.0* for more information on configuring your FortiOS device.

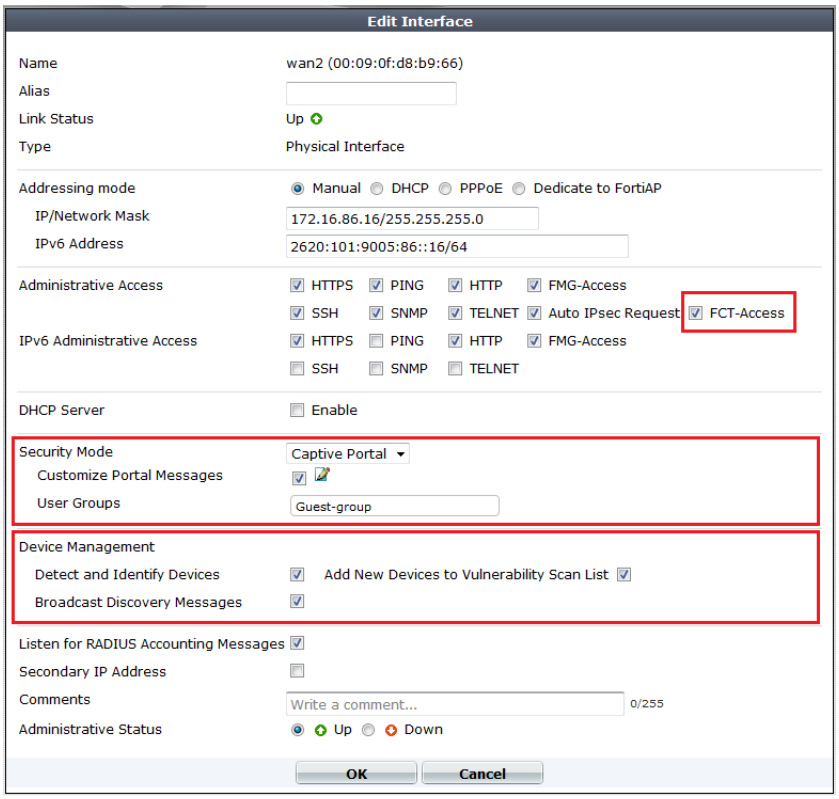
Configure Endpoint Management on the FortiOS device:

1. Enable device management and broadcast discovery messages.

   To configure *Device Management,* go to *System* > *Network* > *Interface,* select the interface, and select *Edit* in the toolbar. In the *Edit Interface* page you can select to enable *Detect and Identify Devices.* To enable *Broadcast Discovery Messages* (optional) you must first enable *FCT-Access* under *Administrative Access*. Select *OK* to save the setting.

Broadcast Discovery Messages is an optional configuration. When enabled, the FortiGate will broadcast messages to your network, allowing client connections to discover the FortiGate for FortiClient registration. Without this feature enabled, the user will enter the IP address or URL of the FortiGate to complete registration.

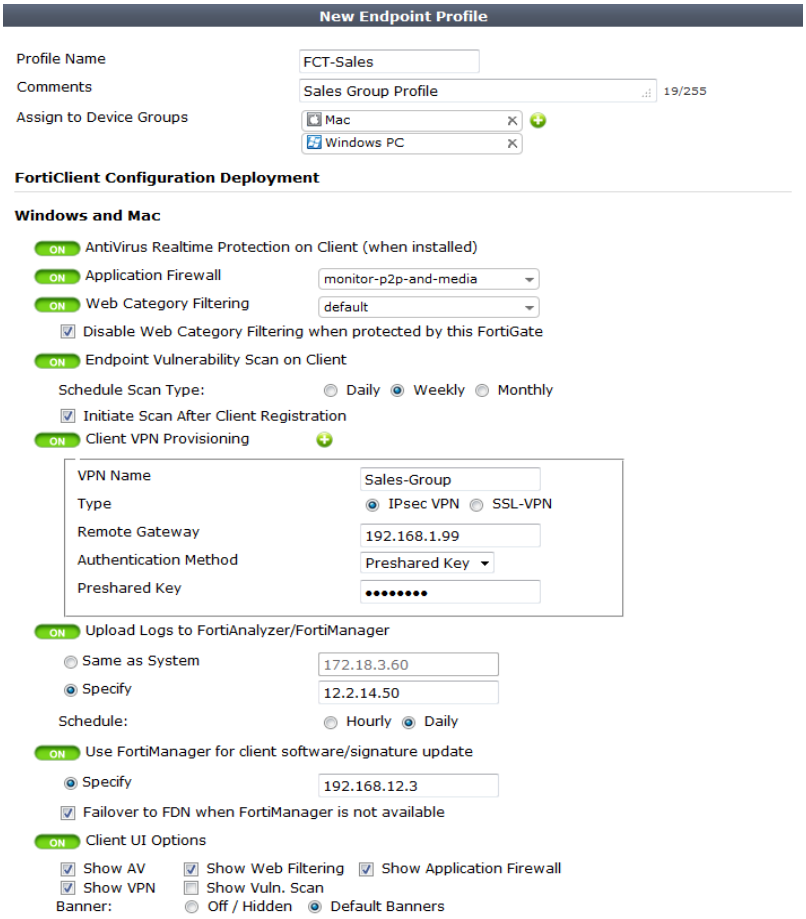
Figure 27: Edit interface window



2. Configure the client endpoint profile.

   To configure the *Client Endpoint Profile*, go to *User & Device* > *Device* > *Endpoint Profile*. You can edit the default profile for create a new endpoint profile.

Figure 28: New endpoint profile window



3. Configure the following settings:

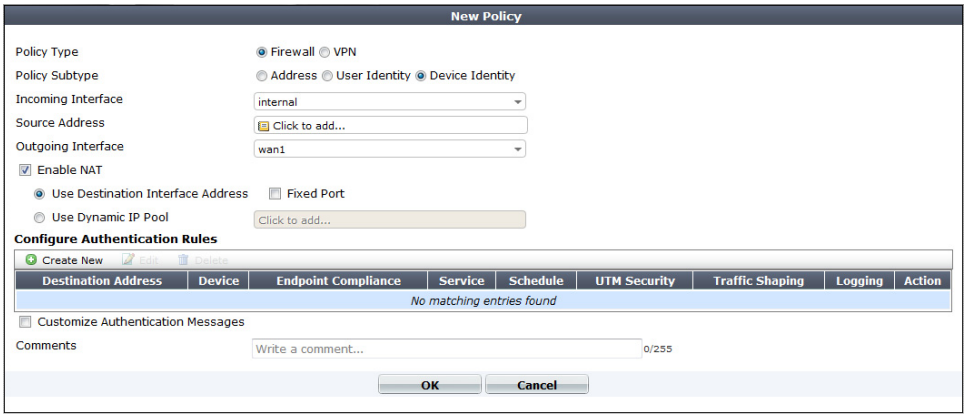
Toolbar Options	Select the endpoint profile using the drop-down menu. Select the plus (+) icon to create a new endpoint profile. Select the view list icon to view endpoint profiles and assignment.
Profile Name	Enter a name for the new endpoint profile.
Comments	Enter a profile description. (optional)
Assign to Device Groups	Use the plus (+) icon to assign multiple device groups, for example Mac and Windows PC.
Antivirus Real time Protection on Client (when installed)	Toggle the button on or off.
Application Firewall	Toggle the button on or off. When enabled, you can select an application firewall profile in the drop-down menu.
Web Category Filtering	Toggle the button on or off. When enabled, you can select a web category filtering profile in the drop-down menu. Select the checkbox to disable web category filtering on the client when protected by the FortiGate.

Endpoint Vulnerability Scan on Client	Toggle the button on or off. When enabled, you can select the scheduled scan type to daily, weekly, or monthly. Select the checkbox to initiate a scan after client registration with the FortiGate.
Client VPN Provisioning	Toggle the button on or off. When enabled, you can configure multiple IPsec and SSL VPN connections. Select the plus (+) icon to add additional VPN connections. Enter the VPN name, type, remote gateway, and authentication method information.
Upload Logs to FortiAnalyzer/FortiManager	Toggle the button on or off. When enabled, you can select to use the same FortiAnalyzer/FortiManager used by the FortiGate or select Specify to enter a different device IP. You can set the schedule to hourly or daily. The FortiClient upload logs to the FortiAnalyzer/FortiManager only when it is able to connect to the device on the specified IP address.
Use FortiManager for client software/signature update	Toggle the button on or off. When enabled, you can specify the IP address of the FortiManager. Select the checkbox to failover to the FortiGuard Distribution Network when the FortiManager is not available.
Client UI Options	Toggle the button on or off. When enabled, you can select which FortiClient modules are visible in the FortiClient console window. Select the appropriate checkbox to show the module.

4. Select *OK* to save the endpoint profile setting.
5. Configure firewall policies for the endpoint profile.

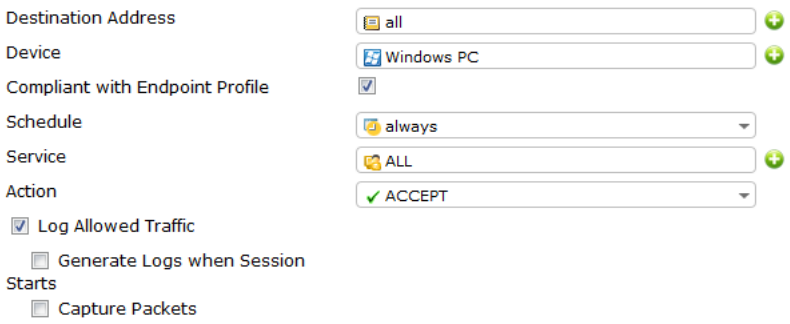
   To configure a firewall policy for *Endpoint Management*, go to *Policy* > *Policy* > *Policy* and select *Create New* in the right-hand toolbar. For *Policy Subtype*, select *Device Identity*.

Figure 29: New policy window



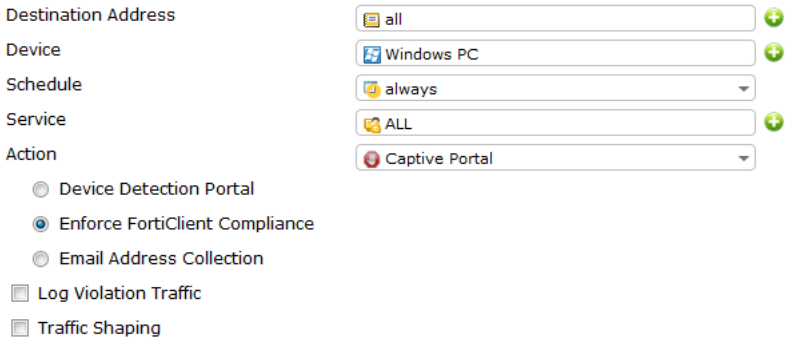
Add an *Accept* authentication rule for all compliant Windows-PC clients. This rule will allow Windows clients which have installed FortiClient and have been registered to this FortiGate to pass traffic.

Figure 30: Accept authentication rule for compliant Windows-PC clients.



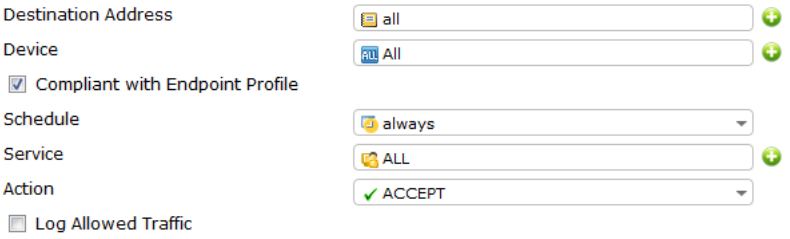
Add a *Captive Portal* authentication rule for all non-compliant Windows-PC clients. This rule will redirect all Windows clients (via a web browser) to a dedicated portal where they can download the client. Once registered to the FortiGate, the endpoint profile will be assigned.

Figure 31: Captive portal authentication rule for Windows-PC devices.



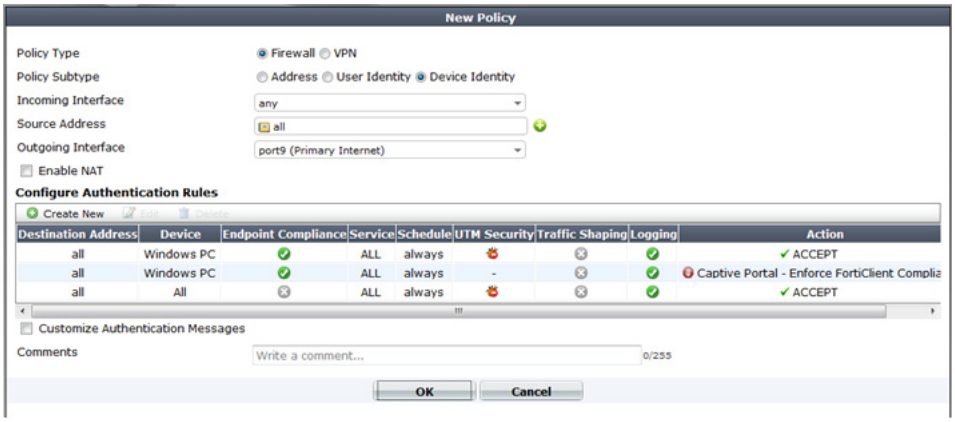
(Optional) Add an *Accept* authentication rule to allow traffic from all other devices to pass traffic without enforcing FortiClient Compliance.

Figure 32: Accept authentication rule for all other devices



Once these three authentication rules are configured, select *OK* to save the new policy setting. Your client configuration is ready for deployment.

Figure 33: New policy window



After the FortiGate configuration has been completed, you can proceed with FortiClient configuration. Configure your Windows PC on the corporate network with the default gateway set to the IP of the FortiGate.

FortiClient endpoint network topologies

The following FortiClient Endpoint Profile topologies are supported:

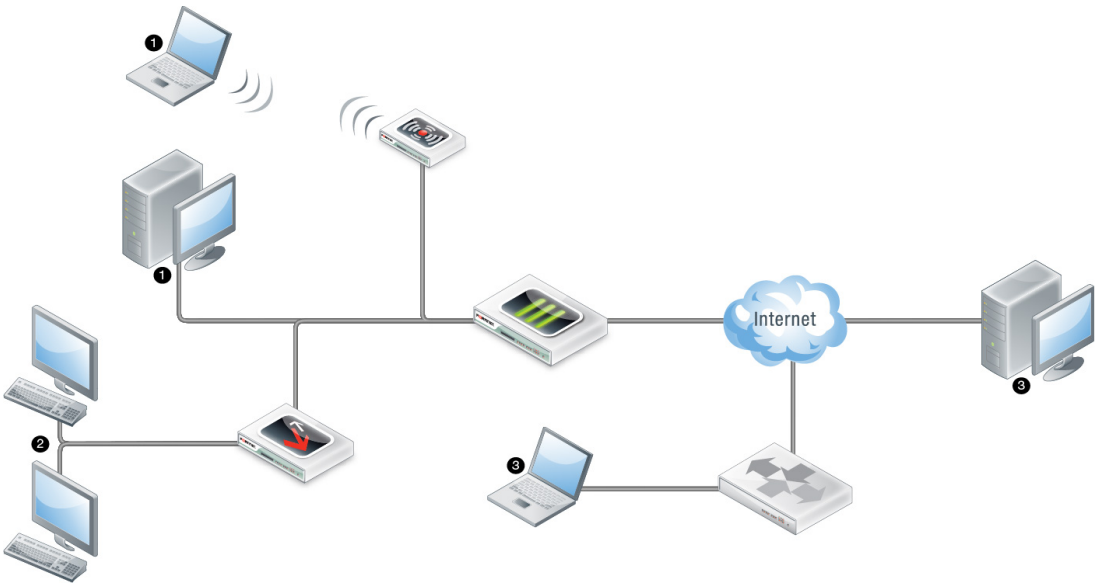
- Client is directly connected to FortiGate; either to a physical port, switch port or WiFi SSID.[1]

  This topology supports client registration, configuration sync, and endpoint profile enforcement.
- Client is connected to FortiGate, but is behind a router or NAT device.[2]

  This topology supports client registration and configuration sync.
- Client is connected to FortiGate across a VPN connection.[3]

  This topology supports client registration, configuration sync, and endpoint profile enforcement.

Figure 34: Network topologies



Configure FortiClient for Endpoint Management:

1. Download and install the FortiClient software.

   Open a web browser from your workstation and attempt to open a web page, the web page will be directed to the Captive Portal. Follow the instructions in the portal to download and install FortiClient.

To allow users to download FortiClient, you must enable this setting in the *SSL VPN Portal* on your FortiOS device.

Figure 35: Captive portal block page

Endpoint Security Required

The use of this security policy requires that the latest FortiClient Endpoint Security software is working properly. Please make sure

- *FortiClient is installed and running,*
- *FortiClient is registered with FortiGate and currently in "online" status, and*
- *the "Disable configuration sync with FortiGate" option in FortiClient settings is turned off.*

Installing FortiClient requires that you have administrator privileges on your computer. If you do not, please contact your network administrator to have FortiClient installed.

The installer may be downloaded using the following link:
FortiClientInstaller-Windows-Enterprise-5.0.0.exe

Installation instructions:

- *For Internet Explorer:*
  1. Click the above link to download the installer
  2. When Internet Explorer asks what action you would like to take, click "Run"
- *For Firefox:*
  1. Click the above link to download the installer
  2. Save the installer and note the location it is saved to
  3. Open the folder containing the installer and run it

FortiClient installation may take a few minutes. Thank you for your patience.

2. Register FortiClient.

   After FortiClient completes installation, FortiClient will automatically launch and search for a FortiGate device for registration.

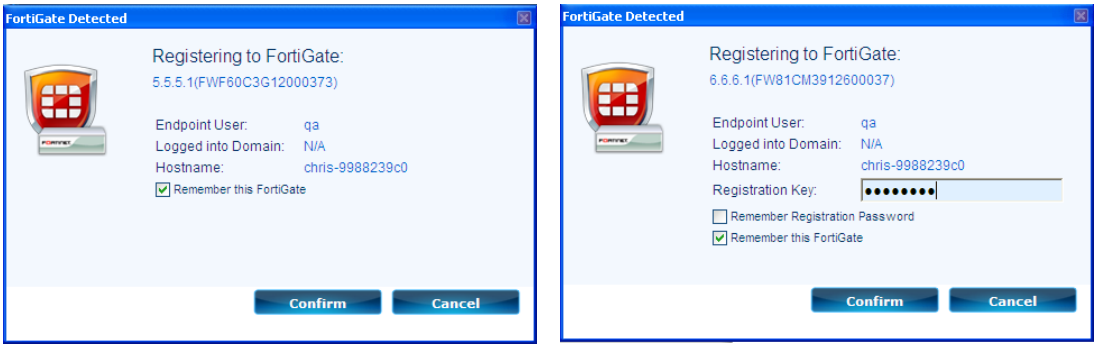
   There are three ways that the FortiClient/FortiGate communication is initiated:

   - FortiClient connects to the preferred IP address (if provided).
   - If the first option fails, FortiClient will attempt to connect to the default gateway IP address.
   - If the first two option fail, FortiClient will listen for FortiGate broadcast messages.

Your personal computer's default gateway IP should be configured to be the IP set in the FortiGate interface.

FortiClient will search for available FortiGate devices to complete registration. You can include the option to prompt the user to enter the FortiClient registration key. Select the *FortiGate* icon in the FortiClient console to retry the search.

Figure 36: FortiGate detected confirmation dialog boxes

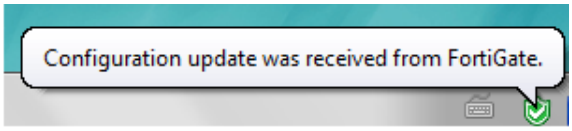


If FortiClient is unable to detect a FortiGate device, enter the IP address or URL of the device and select the *Retry* button. When FortiClient locates the FortiGate, you will be prompted to confirm the registration. Select the *Confirm* button to complete registration. Upon successful registration, the FortiGate will deploy the endpoint configuration.

3. Deploy the endpoint profile from the FortiOS device.

   The FortiGate will deploy the endpoint profile after registration is complete. This endpoint profile will permit traffic through the FortiGate. A system tray bubble message will be displayed once update is complete.

Figure 37: Configuration update notification message



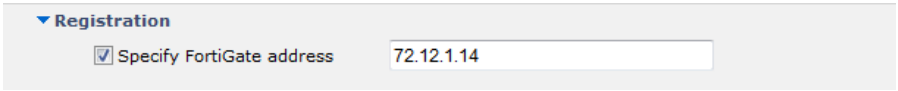
The FortiClient console will display that it is successfully registered to the FortiGate. The endpoint profile is installed on FortiClient.

Figure 38: Registered FortiClient console

Deploy the endpoint profile to clients over a VPN connection:

1. In the FortiClient console, select *File* > *Settings*. Under *Registration* select *Specify FortiGate address* and enter the IP address and port number (if required) of the FortiGate's internal interface.

   Figure 39: Preferred FortiGate address

2. Configure an IPsec VPN connection from FortiClient to the management FortiGate. For more information on configuring IPsec VPN see "Create a new IPsec VPN connection" on page 65.
3. Connect to the VPN.
4. You can now search for the FortiGate gateway. See "Register FortiClient." on page 41 for more information.
5. After registration, the client is able to receive the endpoint profile.

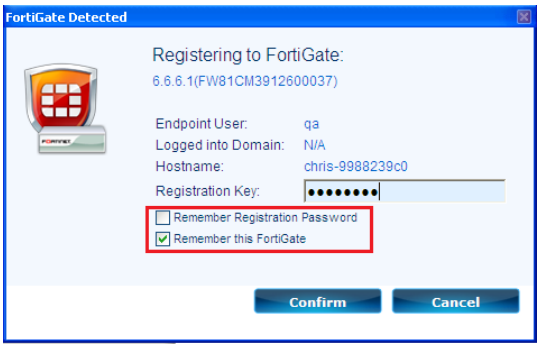
When creating a new FortiClient VPN (IPsec) or SSL VPN tunnel configuration on your FortiOS device, you must enable *Endpoint Registration*. See the *IPsec VPN for FortiOS 5.0* and *SSL VPN for FortiOS 5.0* sections of the *FortiOS 5.0 Handbook* for more information.

Remembered FortiGates

FortiClient v5.0 Patch Release 1 or later adds the option to remember up to 20 FortiOS devices when accepting the broadcast registration message. FortiClient can remember and register to multiple FortiOS devices. This feature enables users to move freely between office locations and register conveniently to each FortiGate device.

When prompted to enter a registration key, FortiClient can remember the registration password.

Figure 40: Option to remember FortiGate



Select the registration icon in the console to view information for the current registered device including the hostname, domain, serial number, and IP address.

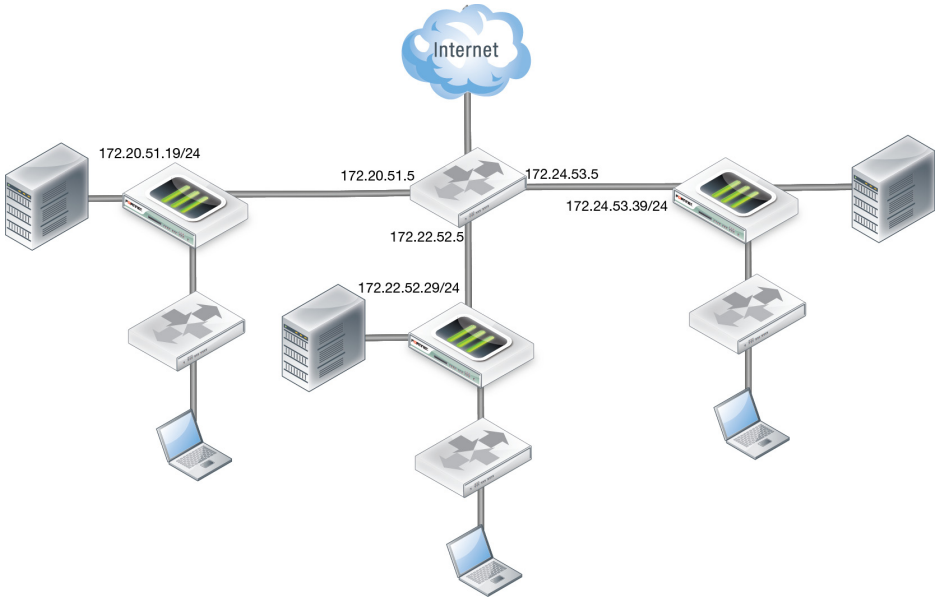
Figure 41: Remembered FortiGates

Select *Remembered FortiGates* to show a list of FortiGate devices that FortiClient has previously registered with. Use the right-click menu to forget a specific device. Select the device that you would like to remove from the remembered FortiGates list, right-click, and select *Forget.* You can also change the order of devices in this list using the right-click menu.

Roaming clients (multiple redundant gateways) example

The following figure illustrates three corporate FortiGate networks. Each FortiGate can reach each other over a WAN network. FortiClient can only reach one FortiGate at a time. FortiClient may connect directly to the FortiGate or through a NAT device.

Figure 42: Roaming clients topology



If FortiClient connects through a NAT device to the FortiGate, do not enforce endpoint control compliance on the FortiGate.

On each of the three FortiGate devices configure the following:

- Interface IP addresses
- Endpoint control profile
- Device identification in the interface
- Endpoint control profile in the applicable firewall policy
- Endpoint control synchronization

Endpoint control synchronization allows you to synchronization endpoint control for multiple FortiGate devices. To enable endpoint control synchronization via the CLI enter the following commands on your FortiGate:

```
config endpoint-control forticlient-registration-sync
  edit 1
    set peer-ip 172.20.52.19
    next
    edit 2
    set peer-ip 172.22.53.29
  end
end
```

The IP addresses set for the peer-ip field are the WAN IP addresses for each of the FortiGate devices in the synchronization group.

You need to add the following XML configuration to FortiClient for this synchronization group. Modify the configuration file to add the following:

```
<forticlient_configuration>
  <endpoint_control>
    <!-- List of redundant FortiGates, since 5.0.2 -->
    <fortigates>
      <fortigate>
        <name>Corporate Network</name>
        <addresses>10.18.51.9;10.20.52.19;10.22.53.29</addresses>
      </fortigate>
    </fortigates>
  </endpoint_control>
</forticlient_configuration>
```

The IP addresses are the internal IP addresses for each of the three FortiGates in the synchronization group. FortiClient can reach any of these IPs, one at a time.

If the three FortiGate devices share the same DNS name, use the following XML configuration:

```
<forticlient_configuration>
  <endpoint_control>
    <!-- List of redundant FortiGates, since 5.0.2 -->
    <fortigates>
      <fortigate>
        <name>Fortinet Americas</name>
        <addresses>fct_americas.fortinet.com</addresses>
      </fortigate>
    </fortigates>
  </endpoint_control>
</forticlient_configuration>
```

The DNS server should return one reachable FortiGate IP address for the domain name used.

You will need to manually add FortiClient to the synchronization group when FortiClient initially registers with the FortiGate. Once added, no further action is required.

On your FortiGate, use the following CLI command to list all registered FortiClients:

```
# diagnose endpoint registration list
   FortiClient #1:
    UID                      = BA0FA25998FD4EB3A81072DC3E1799F4
    vdom                     = root
    status                   = registered
    registering time         = Tue Mar  5 15:41:36 2013
    registration expiry time = Tue Mar 12 15:41:36 2013
    source IP                = 192.168.10.100
    user                     = lindseyk
    host OS                 = Microsoft Windows 7 Enterprise Edition,
        64-bit Service Pack 1 (build 7601)
    local registration       = no
    remote registration SN   = FG10DH3G11604696
```

The `local registration` entry indicates whether this specific FortiClient is registered to this FortiGate, or to another FortiGate within the synchronization group.

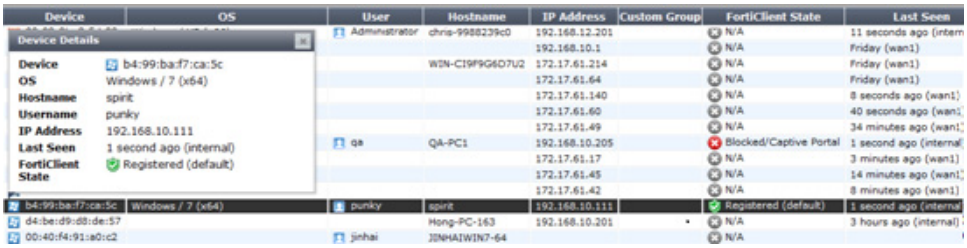
If any of the FortiGate devices require a password to complete registration, you can use the following XML configuration to provide password information to FortiClient:

```
<forticlient_configuration>
   <endpoint_control>
      <!-- List of redundant FortiGates, since 5.0.2 -->
      <fortigates>
         <fortigate>
            <name>Corporate Network</name>
            <addresses>10.18.51.9;10.20.52.19;10.22.53.29</addresses>
            <registration_password>uNbre@kab1e</registration_password>
         </fortigate>
      </fortigates>
   </endpoint_control>
</forticlient_configuration>
```

View FortiClient registration in the FortiGate Web-based Manager

You can view all registered FortiClient agents in the FortiGate Web-based Manager. Each new registration will be automatically added to the device table. To view registered devices go to *User & Devices* > *Device* > *Device Definition*. The state for the new FortiClient registration is listed as *Registered*.

Figure 43: FortiGate device

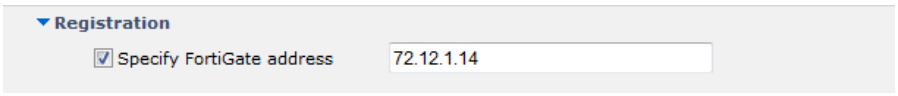


Configure preferred FortiGate IP on FortiClient for registration

The FortiClient admin user can specify a preferred FortiGate IP address for registration and client configuration management. When an unregistered FortiClient starts up, it first looks for the preferred FortiGate. If the preferred FortiGate is not reachable, it will look to connect to default gateway. If both the preferred FortiGate and default gateway are not reachable, FortiClient will listen for the broadcast message from FortiGate.

To configure a preferred FortiGate IP address in FortiClient, select *File* > *Settings.* Select *Registration* to expand the drop-down menu. Enter the IP address and port number (if required) of the FortiGate's internal interface.

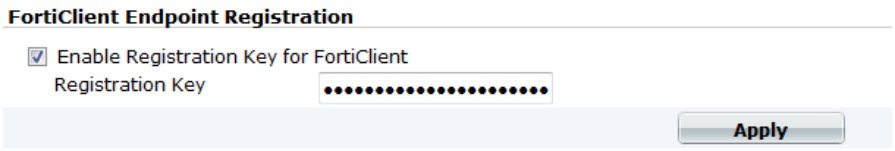
Figure 44: Configure preferred FortiGate in FortiClient



Enable FortiClient endpoint registration (optional)

To enable *FortiClient Endpoint Registration* in the FortiOS Web-based Manager, select *System* > *Config* > *Advanced*. Select *Enable Registration Key for FortiClient*, enter the *Registration Key* and select *Apply*.

Figure 45: Enable FortiClient endpoint registration on FortiGate



The FortiClient user will need to enter the same registration key to successfully register FortiClient to the FortiGate.

Antivirus

FortiClient Antivirus

FortiClient v5.0 includes an antivirus module to scan system files, executables, dll's, and drivers. FortiClient will also scan for and remove rootkits.

This section describes how to enable antivirus and configuration options.

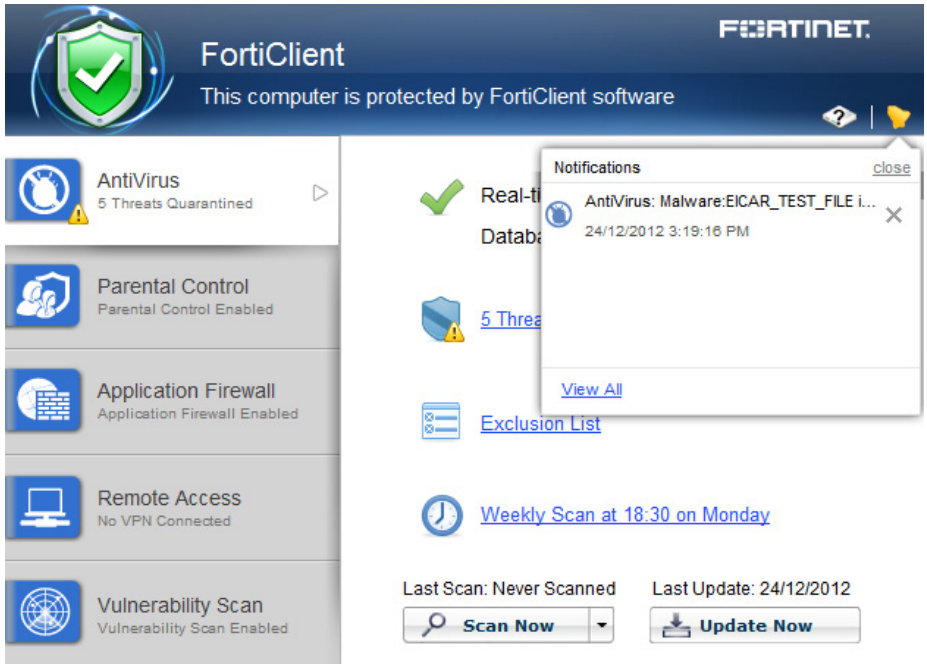
Enable/disable antivirus

To enable or disable FortiClient antivirus real-time protection, toggle the *[Enable/Disable]* option in the FortiClient console.

Notifications

Select the bell icon in the FortiClient console to view all notifications. When a virus has been detected, an exclamation (!) icon will appear in the antivirus tree-menu tab. The bell icon will change from gray to yellow. Select *View All* to view all antivirus event notifications.

Figure 46: Antivirus notifications dialog box



Scan now

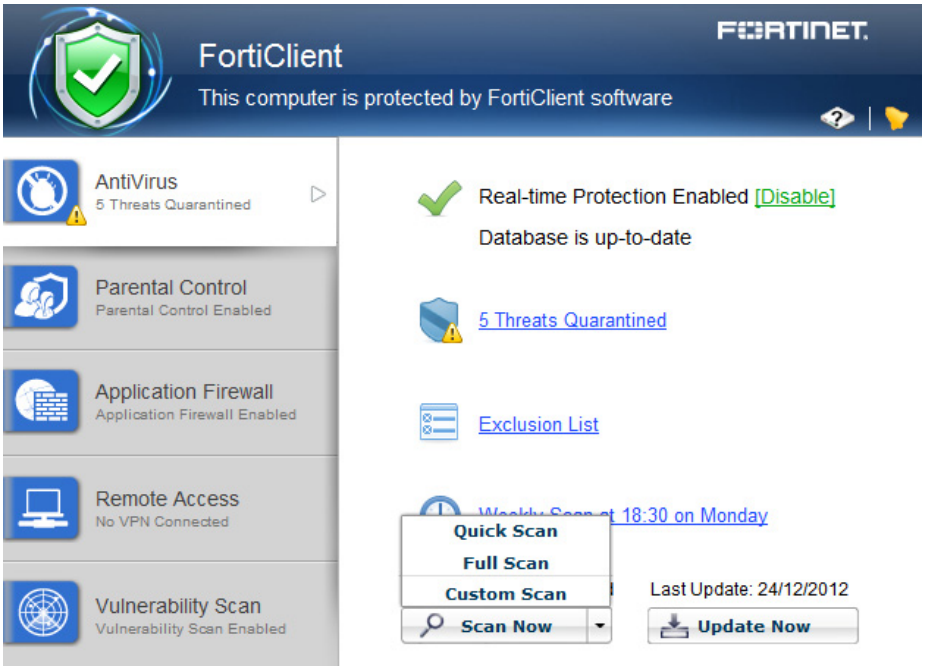
To perform on-demand antivirus scanning, select the *Scan Now* button in the FortiClient console. Use the drop-menu to select *Custom Scan, Full Scan*, or *Quick Scan*. The console displays the date of the last scan above the button.

Custom Scan runs the rootkit detection engine to detect and remove rootkits. *Custom Scan* allows you to select a specific file folder on your local hard disk drive (HDD) to scan for threats.

Full Scan runs the rootkit detection engine to detect and remove rootkits. *Full Scan* then performs a full system scan including all files, executables, dll's, and drivers for threats.

Quick System Scan runs the rootkit detection engine to detect and remove rootkits. *Quick System Scan* only scans executable files, dll's, drivers that are currently running for threats.

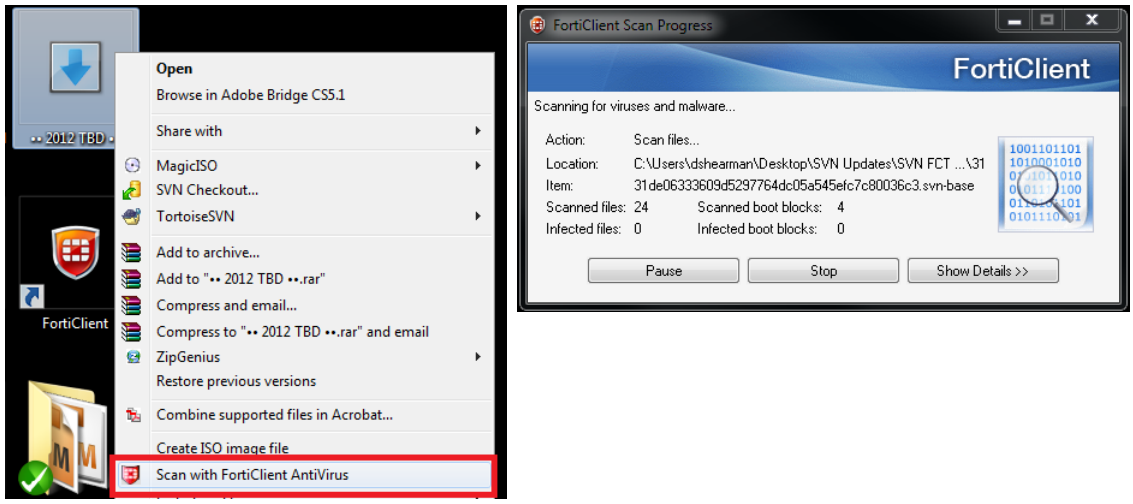
Figure 47: Antivirus scan options



Scan a file or folder on your workstation

To perform a virus scan a specific file or folder on your workstation, right-click the file or folder and select *Scan with FortiClient AntiVirus*.

Figure 48: Scan a specific file or folder



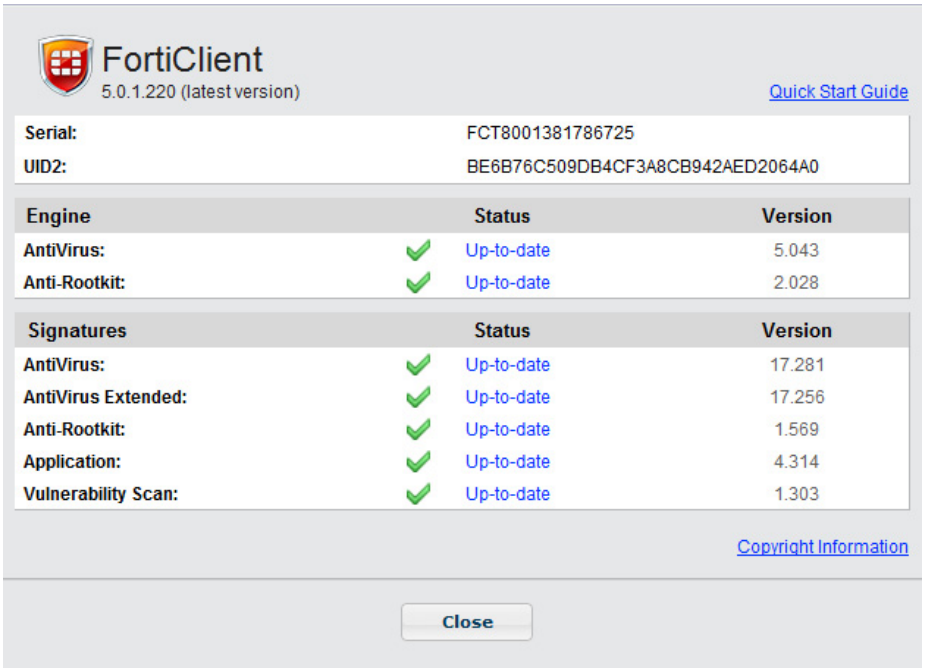
Update now

To perform on-demand update of FortiClient version, engines, and signatures, select the *Update Now* button in the FortiClient console. The console notes the date of the last update above the button.

To view the current FortiClient version, engine, and signature information, select *Help* in the toolbar, and select *About* in the drop-down menu.

You can select to use a FortiManager device for client software and signature updates. When configuring the endpoint profile, select *Use FortiManager for client software/signature updates* to enable the feature and enter the IP address of your FortiManager device.

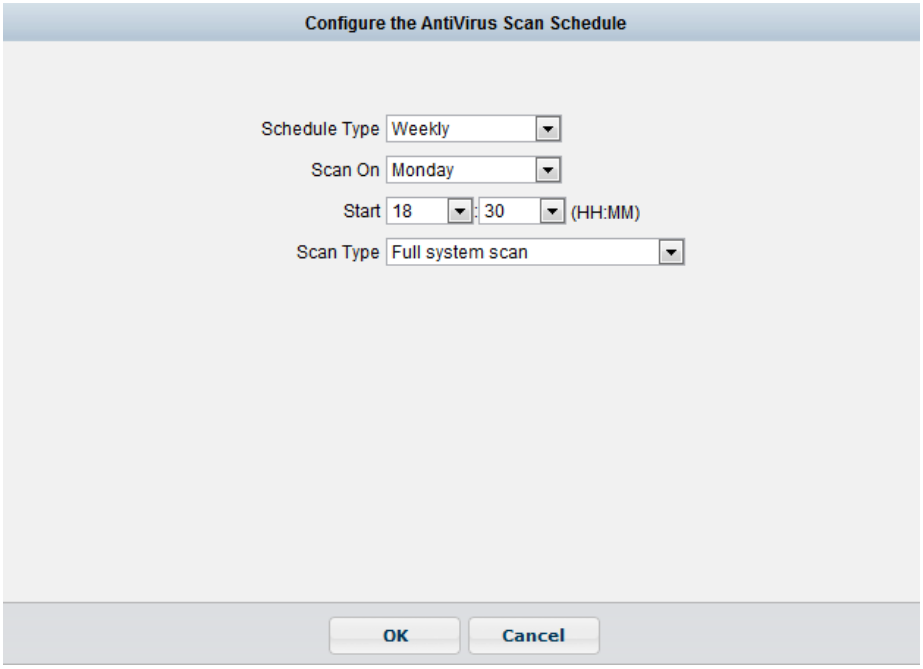
Figure 49: About FortiClient page



Schedule antivirus scanning

To schedule antivirus scanning, select *Weekly Scan* in the content pane.

Figure 50: Antivirus scheduling



Configure the following settings:

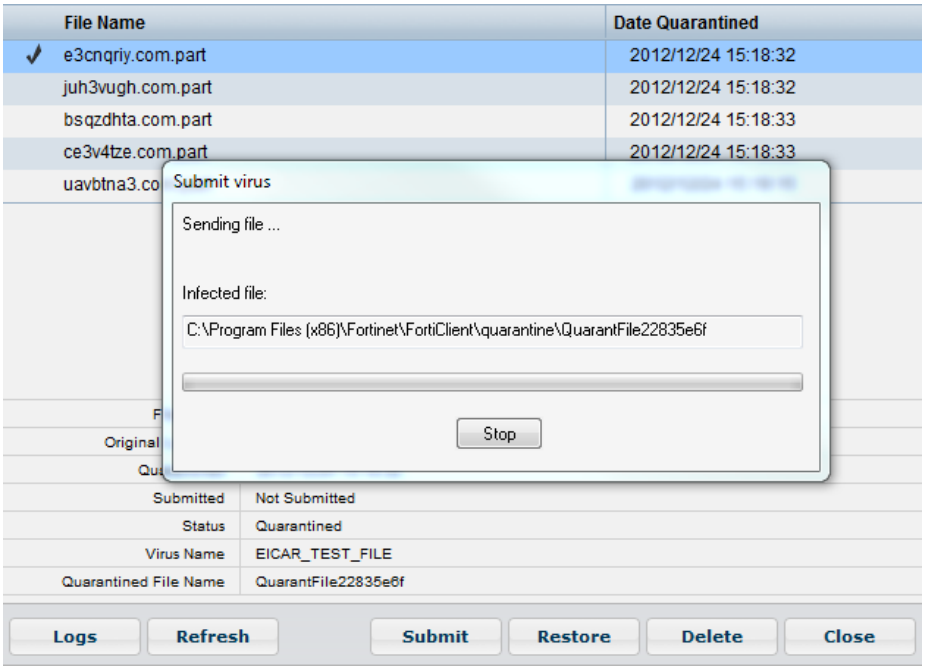
Schedule Type	Select Daily, Weekly or Monthly in the drop-down menu.
Scan On	For Weekly scheduled scan, select the day of the week in the drop-down menu. For Monthly scheduled scan, the day of the month in the drop-down menu.
Start	Select the start time in the drop-down menus. The time format is represented in hours and minutes, 24-hour clock.
Scan Type	Select the scan type: ***Custom Scan*** runs the rootkit detection engine to detect and remove rootkits. *Custom Scan* allows you to select a specific file folder on your local hard disk drive (HDD) to scan for threats. ***Full Scan*** runs the rootkit detection engine to detect and remove rootkits. *Full Scan* then performs a full system scan including all files, executables, dll's, and drivers for threats. ***Quick System Scan*** runs the rootkit detection engine to detect and remove rootkits. *Quick System Scan* only scans executable files, dll's, drivers that are currently running for threats.

Select *OK* to save the setting.

View quarantined threats

To view quarantined threats, select *Threats Quarantined* in the FortiClient console. In this page you can view, restore, or delete the quarantined file. You can also submit the file to FortiGuard.

Figure 51: Threats quarantined page



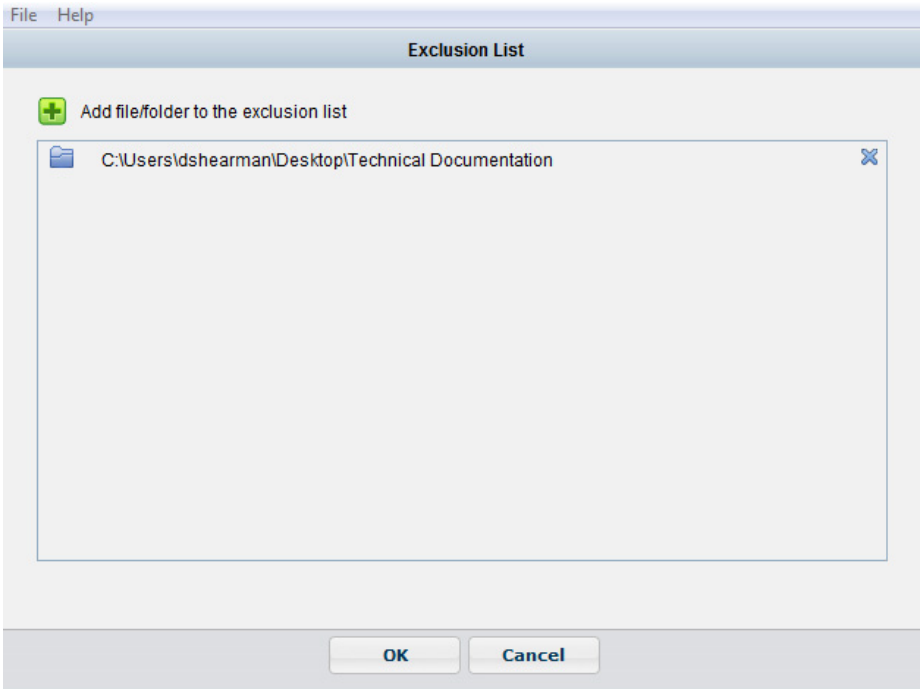
This page displays the following:

File Name	The name of the file.
Date Quarantined	The date and time that the file was quarantined by FortiClient.
File Information	Select a file from the list to view detailed information including the quarantined location, status, virus name, and quarantined file name.
Logs	Select to view FortiClient log data.
Refresh	Select to refresh the list.
Submit	Select to submit the quarantined file to FortiGuard.
Restore	Select to add the selected file/folder to the exclusion list.
Delete	Select to delete the quarantined file.
Close	Select to close the page and return to the FortiClient console.

Add files/folders to an exclusion list

To add files/folders to the antivirus exclusion list, select *Exclusion List* in the content pane. In the following configuration page, select the plus '+' symbol to add files or folders to the list. Any files or folders in this exclusion list will not be scanned.

Figure 52: Antivirus exclusion list page

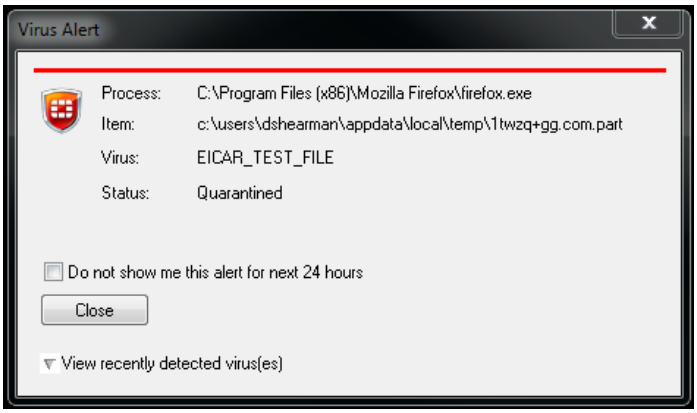


Select *OK* to save the setting.

Antivirus warning

When FortiClient antivirus detects a virus while attempting to download a file via a web-browser, you will receive a warning dialog message similar to Figure 53. Browse to the *Threat Quarantine* menu in the console to view details for the detected threat.

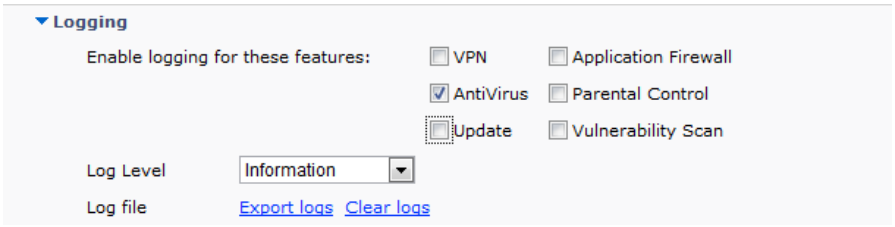
Figure 53: Example virus warning message



Antivirus logging

To configure antivirus logging, select *File* in the toolbar and *Settings* in the drop-down menu. Select *Logging* to view the drop-down menu.

Figure 54: Logging options



Configure the following settings:

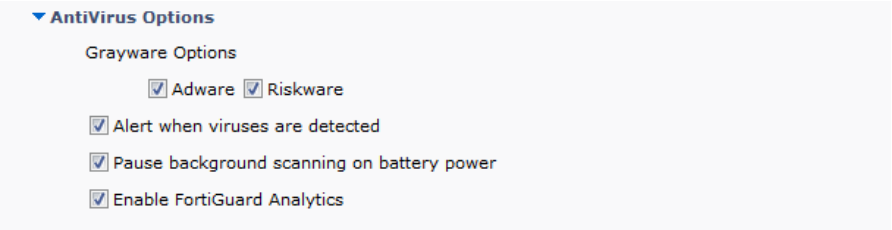
Logging	
Enable logging for these features	Select antivirus to enable logging for this feature.

Log Level	Select the level of logging: **Emergency:** The system becomes unstable. **Alert:** Immediate action is required. **Critical:** Functionality is affected. **Error:** An error condition exists and functionality could be affected. **Warning:** Functionality could be affected. **Notice:** Information about normal events. **Information:** General information about system operations. **Debug:** Debug FortiClient.
Log file	
Export logs	Select to export logs to your local hard disk drive (HDD) in .log format.
Clear logs	Select to clear all logs. You will be presented a confirmation window, select *Yes* to proceed.

Antivirus options

To configure antivirus options, select *File* in the toolbar, and *Settings* in the drop-down menu. Select *AntiVirus Options* to view the drop-down menu. In this menu you can configure options outlined in the following figure and table.

Figure 55: Antivirus options



Configure the following settings:

Antivirus Options	
Grayware Options	Grayware is an umbrella term applied to a wide range of malicious applications such as spyware, adware and key loggers that are often secretly installed on a user's computer to track and/or report certain information back to an external source without the user's permission or knowledge.
Adware	Select to enable adware detection and quarantine during the antivirus scan.
Riskware	Select to enable riskware detection and quarantine during the antivirus scan.

Alert when viruses are detected	Select to have FortiClient provide a notification alert when a threat is detected on your personal computer.
Pause background scanning on battery power	Select to pause background scanning when your personal computer is operating on battery power.
Enable FortiGuard Analytics	Select to automatically send suspicious files to the FortiGuard Network for analysis.

Parental Control/Web Filtering

FortiClient Parental Control/Web Filtering

Parental Control/Web Filtering allows you to block, allow, warn, and monitor web traffic based on URL category. URL categorization is handled by the FortiGuard Network.

When FortiClient is registered to a FortiGate, the *Parental Control* module will reflect *Web Filtering*. You can disable *Web Category Filtering* in FortiClient from the FortiGate endpoint profile. If the FortiClient device is behind a FortiGate, the client device will use the web filter profile from the FortiGate.

Enable/Disable Parental Control/Web Filtering

To enable or disable FortiClient Parental Control/Web Filtering, toggle the *[Enable/Disable]* button in the FortiClient console. Parental Control is enabled by default.

Figure 56: Parental control module

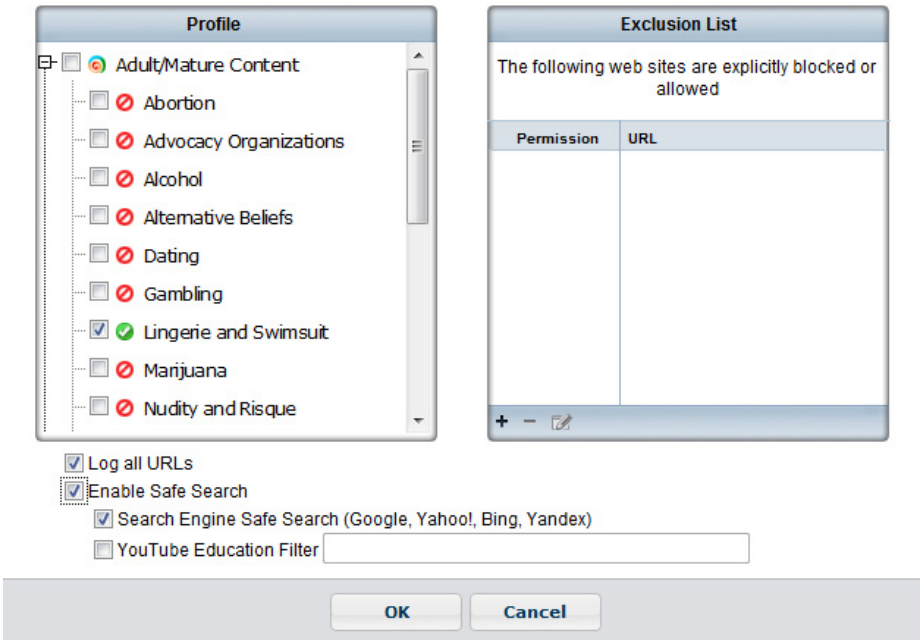
Enable/Disable	Toggle to enable or disable Parental Control.
Settings	Select to configure the Parental Control profile.

Parental Control/Web Filtering settings

You can configure a profile to allow, block, warn, or monitor web traffic based on category under *Profile*. Use the right-click menu to set the action for the full category or sub-category.

You can add websites to the exclusion list and set the permission to allow or block. If the website is part of a blocked category, an allow permission in the *Exclusion List* would allow the user to access the specific URL.

Figure 57: Profile and exclusion list



Configure the following settings:

Profile	Select to allow, block, warn or monitor traffic by category or sub-category.
Exclusion List	Select to exclude websites that are explicitly blocked or allowed. Use the plus (+) icon to add websites and the minus (-) icon to delete websites from the list.
Log all URLs	Select to log all URLs.
Enable Safe Search	Select to enable safe search.
Search Engine Safe Search	Select to enable search engine safe search for Google, Yahoo, Bing, and Yandex.
YouTube Education Filter	Select to enable the YouTube educational filter and enter your filter code. The filter blocks non-educational content as per your YouTube filter code.

See http://support.google.com/youtube/bin/answer.py?hl=en&answer=2592715 for more information on YouTube for schools and the education filter.

View profile violations

To view profile violations, select *Violations (in the Last 7 Days)* in the FortiClient console.

Figure 58: Traffic violations

Website	Category	Time	User
ffupdate.conduit-services.com	Malicious Websites	25/10/2012 9:53:37 AM	dshearman

Application Firewall

FortiClient application firewall

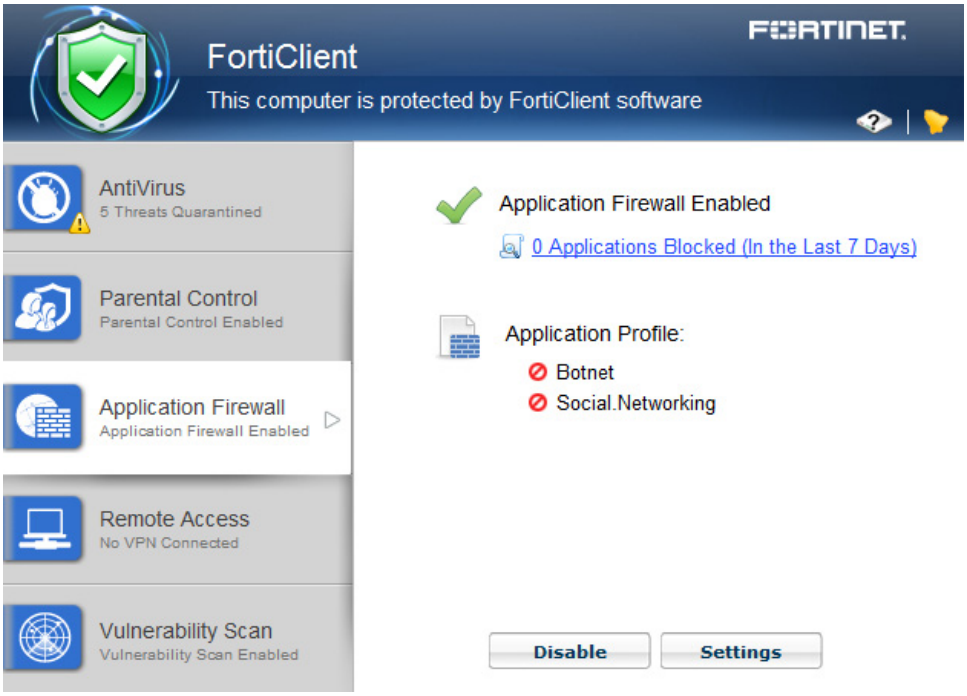
FortiClient v5.0 can recognize the traffic generated by a large number of applications. You can create rules to block or allow this traffic per category, or application.

This section describes how to enable the application firewall settings.

Enable/Disable application firewall

To enable or disable the *FortiClient Application Firewall*, select the *[Enable/Disable]* button in the FortiClient console.

Figure 59: Application firewall module



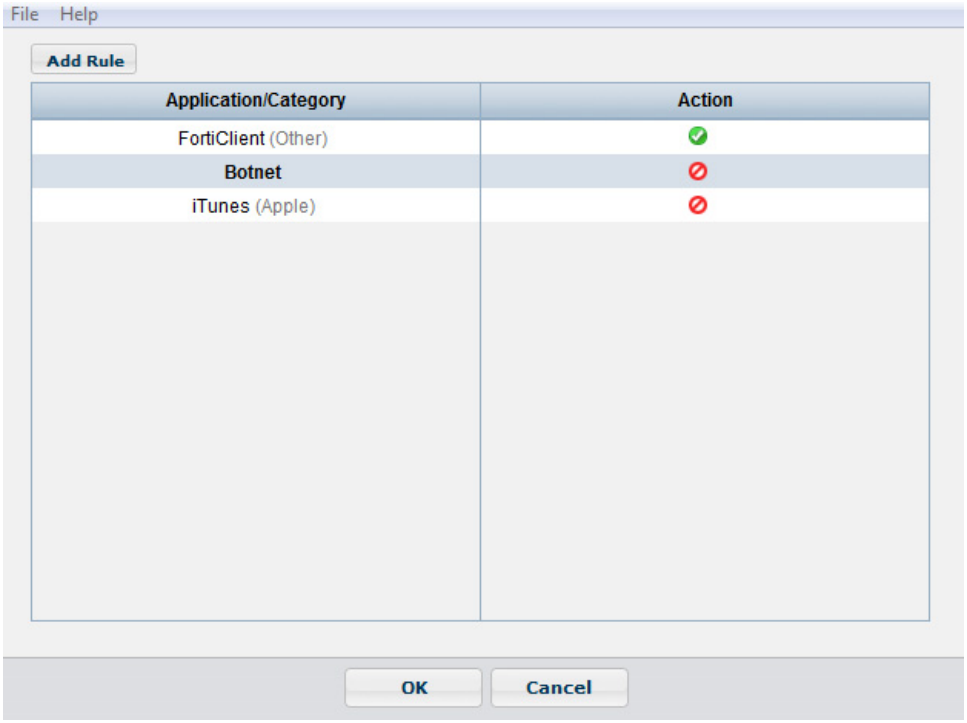
View applications blocked

To view blocked applications, select *Applications Blocked* in the FortiClient console. This page lists all applications blocked in the past seven days, including the count and time of last occurrence.

Application firewall rules

To view Application Firewall rules, select the *Settings* button in the FortiClient console.

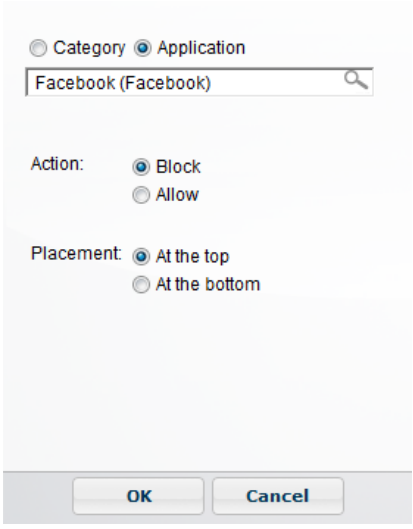
Figure 60: Application Firewall rules



To add a new rule:

1. Select the *Add Rule* button.

Figure 61: Add rule window



2. Select either *Category* or *Application*. For category, use the drop-down list to select a category. For application, type either the full name of the application or first letter to search all applications starting with the selected letter.

FortiClient Application Firewall can only block applications for which FortiGuard has an application signature. You can submit a request to add a application signature on the FortiGuard site.

3. Select the action to *Block* or *Allow* the category or application.
4. Select placement of the rule *At the top* or *At the bottom*.
5. Select *OK* to save the setting.

To edit a rule:

1. In the *Settings* page, when you hover the mouse cursor on a rule, a hidden icon menu is available.
2. Select the edit icon to change the action of the rule.
3. Select the delete icon to remove the rule.
4. Select the move icon and drag-and-drop the rule to a new position in the list.
5. Select *OK* to save the setting and return to the FortiClient console.

Application firewall logging

To configure Application Firewall logging, select *File* in the toolbar, and select *Settings* in the drop-down menu. Select *Logging* to view the drop-down menu. Select *Application Firewall* the logging menu to enable logging for this module.

IPsec VPN and SSL VPN

FortiClient remote access (VPN)

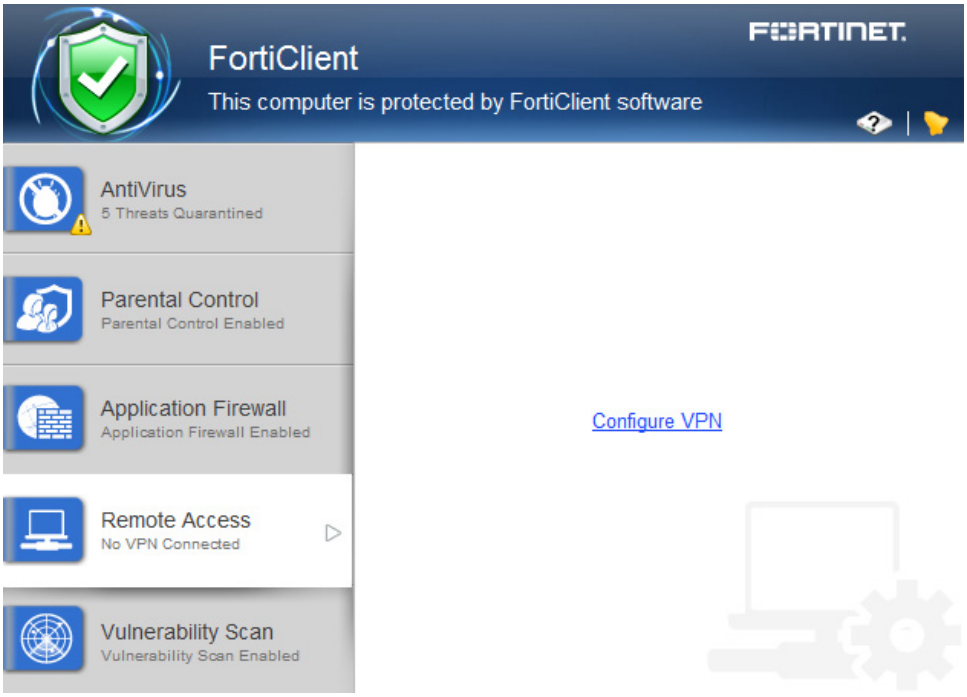
FortiClient v5.0 supports both IPsec and SSL VPN connections to your network for remote access.

This section describes how to configure remote access.

Add a new connection

Select *Configure VPN* in the FortiClient console to add a new VPN configuration.

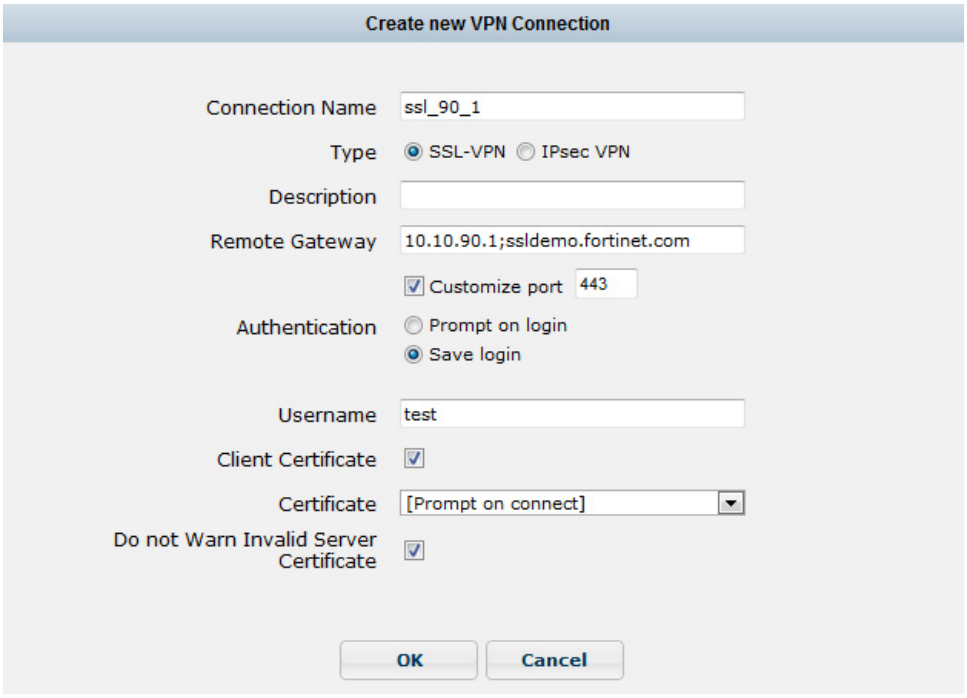
Figure 62: Configure a new VPN connection



Create a new SSL VPN connection

To create a new SSL VPN connection, select *Configure VPN* or use the drop-down menu in the FortiClient console. In this menu you can configure options outlined in the following figure and table.

Figure 63:SSL VPN configuration options



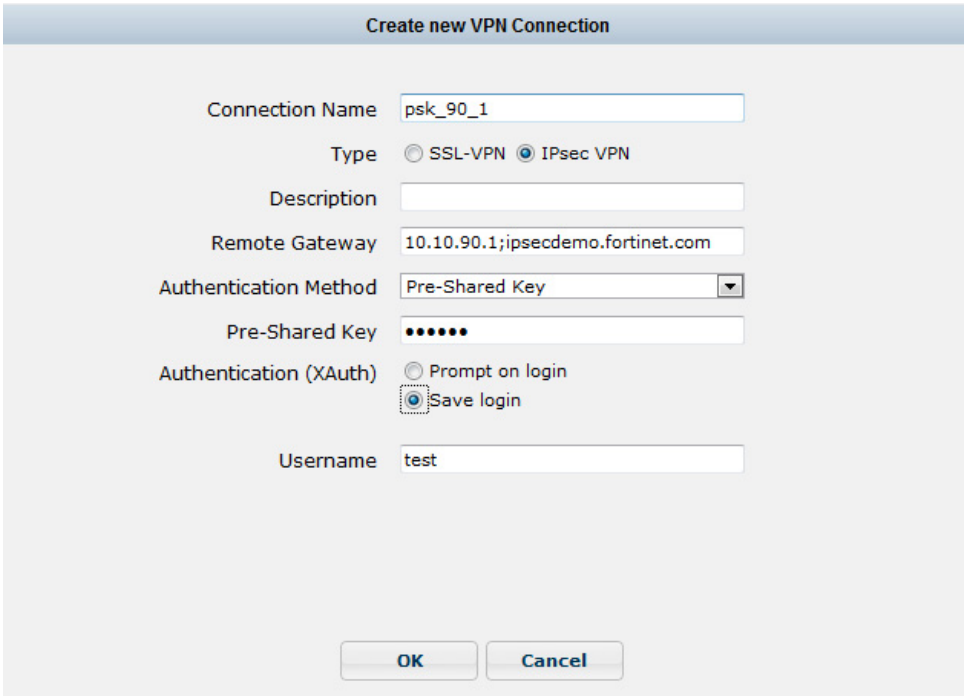
Configure the following settings:

Connection Name	Enter a name for the connection.
Type	Select SSL VPN.
Description	Enter a description for the connection. (optional)
Remote Gateway	Enter the IP address/hostname of the remote gateway. Multiple remote gateways can be configured by separating each entry with a semicolon. If one gateway is not available, the VPN will connect to the next configured gateway.
Port	Select to change the port. The default port is 443.
Authentication	Select to prompt on login, or save login.
Username	If you selected to save login, enter the username in the dialog box.
Client Certificate	Select to enable client certificates.
Certificate	Select the certificate option in the drop-down menu.
Do not warn Invalid Server Certificate	Select if you do not want to warned if the server presents an invalid certificate.

Create a new IPsec VPN connection

To create a new IPsec VPN connection, select *Configure VPN* or use the drop-down menu in the FortiClient console. In this menu you can configure options outlined in the following figure and table.

Figure 64:IPsec VPN configuration options



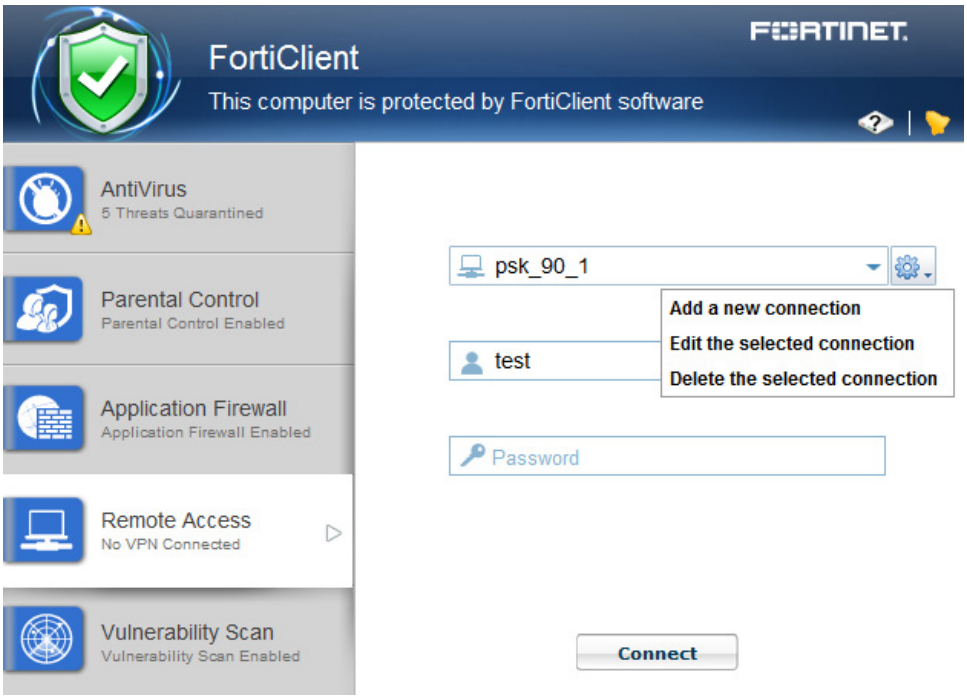
Configure the following settings:

Connection Name	Enter a name for the connection.
Type	Select IPsec VPN.
Description	Enter a description for the connection. (optional)
Remote Gateway	Enter the IP address/hostname of the remote gateway. Multiple remote gateways can be configured by separating each entry with a semicolon. If one gateway is not available, the VPN will connect to the next configured gateway.
Authentication Method	Select either *X.509 Certificate* or *Pre-shared Key* in the drop-down menu.
X.509 Certificate, Pre-shared Key	Select *X.509 Certificate* in the drop-down menu, or enter the pre-shared key in the dialog box. See Certificate Management for information on configuring certificate options.
Authentication (XAuth)	Select to prompt on login, save login, or disable.
Username	If you selected save login, enter the username in the dialog box.

Connect to a VPN

To connect to a VPN, select the name of the VPN from the drop-down menu. Enter your username, password, and select the *Connect* button.

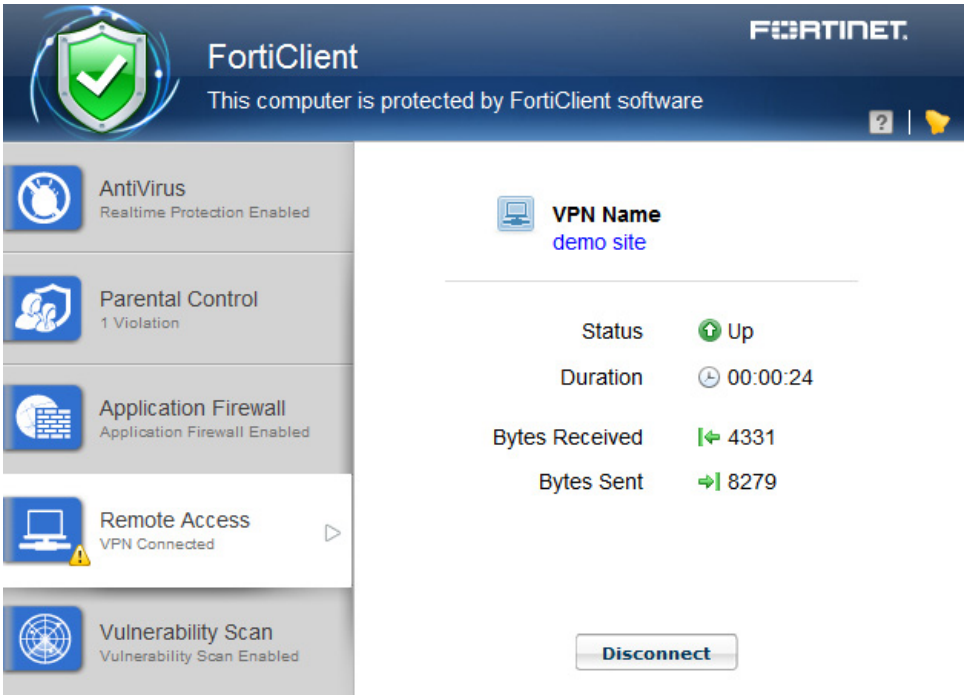
Figure 65: Connection options



You can also select to edit an existing VPN connection and delete an existing VPN connection using the drop-down menu.

When connected, the console will display the connection status, duration, and other relevant information. You can now browse your remote network. Select the *Disconnect* button when you are ready to terminate the VPN session.

Figure 66:SSL VPN connection established



This page displays the following:

Name of the VPN connection	
Status	The status of the VPN connection.
Duration	The duration of the VPN connection.
Bytes Received	Bytes received through the VPN connection.
Bytes Sent	Bytes sent through the VPN connection.
Disconnect	Select to disconnect the VPN connection.

Save Password, Auto Connect, and Always Up (Keep Alive)

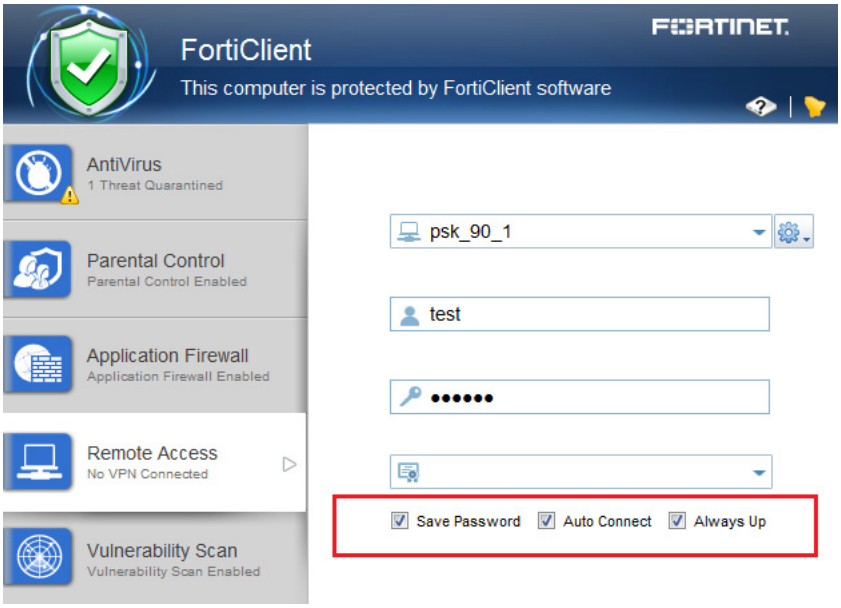
When configuring a FortiClient VPN (IPsec) or SSL VPN connection on your FortiOS device, you can select to enable the following features:

- *Save Password*: Allows the user to save the VPN connection password in the console.
- *Auto Connect*: When FortiClient is launched, the VPN connection will automatically connect.
- *Always Up (Keep Alive)*: When selected, the VPN connection is always up even when no data is being processed. If the connection fails, keep alive packets sent to the FortiGate will sense when the VPN connection is available and re-connect.

For SSL VPN tunnel mode configurations these features are enabled/disabled in the *SSL VPN Portal*.

When enabled in the FortiOS configuration, once the FortiClient is connected to the FortiGate, the client will receive these configuration options.

Figure 67:IPsec VPN console with features enabled



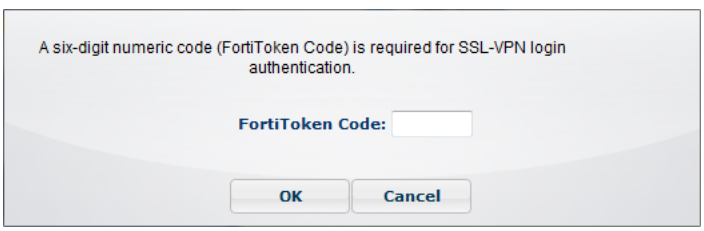
For FortiClient VPN configurations, once these features are enabled they may only be edited from the command line. Use the following commands to disable these features:

```
config vpn ipsec phase1-interface
  edit [vpn name]
    set save-password disable
    set client-auto-negotiate disable
    set client-keep-alive disable
  end
end
```

FortiToken and FortiClient VPN

You can use FortiToken with FortiClient for two-factor authentication. See the *FortiOS 5.0 Handbook* for information on configuring FortiToken, user groups, VPN, and two-factor authentication on your FortiOS device for FortiClient VPN connections.

Figure 68: FortiToken pop-up dialog box



Advanced features (Microsoft Windows)

Connect VPN before logon (AD environments)

The VPN `<options>` tag holds global information controlling VPN states. The VPN will connect first, then logon to AD/Domain.

```
<forticlient_configuration>
  <vpn>
    <options>
      <show_vpn_before_logon>1</show_vpn_before_logon>
      <use_windows_credentials>1</use_windows_credentials>
    </options>
  </vpn>
</forticlient_configuration>
```

Create a redundant IPsec VPN

To use VPN resiliency/redundancy, you will configure a list of FortiGate IP/FQDN servers, instead of just one:

```
<forticlient_configuration>
  <vpn>
    <ipsecvpn>
        <options>
        ...
        </options>
          <connections>
            <connection>
              <name>psk_90_1</name>
              <type>manual</type>
              <ike_settings>
              <prompt_certificate>0</prompt_certificate>
              <server>10.10.90.1;ipsecdemo.fortinet.com;172.17.61
                  .143</server>
              <redundantsortmethod>1</redundantsortmethod>
              ...
          </ike_settings>
        </connection>
      </connections>
    </ipsecvpn>
  </vpn>
</forticlient_configuration>
```

This is a balanced, but incomplete XML configuration fragment. All closing tags are included, but some important elements to complete the IPsec VPN configuration are omitted.

RedundantSortMethod = 1

This XML tag sets the IPsec VPN connection as ping-response based. The VPN will connect to the FortiGate which responds the fastest.

RedundantSortMethod = 0

By default, RedundantSortMethod =0 and the IPsec VPN connection is priority based. Priority based configurations will try to connect to the FortiGate starting with the first in the list.

Priority based SSL VPN connections

SSL VPN supports priority based configurations for redundancy.

```
<forticlient_configuration>
  <vpn>
    <sslvpn>
      <options>
        <enabled>1</enabled>
        ...
      </options>
      <connections>
        <connection>
          <name>ssl_90_1</name>
          <server>10.10.90.1;ssldemo.fortinet.com;172.17.61.143:44
              3</server>
          ...
        </connection>
      </connections>
    </sslvpn>
  </vpn>
</forticlient_configuration>
```

This is a balanced, but incomplete XML configuration fragment. All closing tags are included, but some important elements to complete the SSL VPN configuration are omitted.

For SSL VPN, all FortiGates must use the same TCP port.

Enabling VPN autoconnect

VPN auto connect uses the following XML tag:

```
<autoconnect_tunnel>ipsecdemo.fortinet.com</autoconnect_tunnel>
```

Inside:

```
<vpn>
  <options>
```

Save password is also needed because it is autoconnect:

```
<save_password>1</save_password>
```

Enabling VPN always up

VPN always up uses the following XML tag:

```
<keep_running>1</keep_running>
```

Inside:

```
<vpn>
  <connection>
```

Advanced features (Mac OS X)

Create a redundant IPsec VPN

To use VPN resiliency/redundancy, you will configure a list of FortiGate IP/FQDN servers, instead of just one:

```
<forticlient_configuration>
  <vpn>
    <ipsecvpn>
      <options>
      ...
      </options>
        <connections>
          <connection>
            <name>psk_90_1</name>
            <type>manual</type>
            <ike_settings>
            <prompt_certificate>0</prompt_certificate>
            <server>10.10.90.1;ipsecdemo.fortinet.com;172.17.61
              .143</server>
            <redundantsortmethod>1</redundantsortmethod>
            ...
        </ike_settings>
      </connection>
    </connections>
  </ipsecvpn>
  </vpn>
</forticlient_configuration>
```

This is a balanced, but incomplete XML configuration fragment. All closing tags are included, but some important elements to complete the IPsec VPN configuration are omitted.

RedundantSortMethod = 1

This XML tag sets the IPsec VPN connection as ping-response based. The VPN will connect to the FortiGate which responds the fastest.

RedundantSortMethod = 0

By default, RedundantSortMethod =0 and the IPsec VPN connection is priority based. Priority based configurations will try to connect to the FortiGate starting with the first in the list.

Priority based SSL VPN connections

SSL VPN supports priority based configurations for redundancy.

```
<forticlient_configuration>
  <vpn>
    <sslvpn>
      <options>
        <enabled>1</enabled>
        ...
```

```
            </options>
            <connections>
               <connection>
                  <name>ssl_90_1</name>
                  <server>10.10.90.1;ssldemo.fortinet.com;172.17.61.143:44
                       3</server>
                  ...
               </connection>
            </connections>
         </sslvpn>
      </vpn>
   </forticlient_configuration>
```

This is a balanced, but incomplete XML configuration fragment. All closing tags are included, but some important elements to complete the SSL VPN configuration are omitted.

For SSL VPN, all FortiGates must use the same TCP port.

Enabling VPN autoconnect

VPN auto connect uses the following XML tag:

```
<autoconnect_tunnel>ssl 198 no cert</autoconnect_tunnel>
```

Enabling VPN always up

VPN always up uses the following XML tag:

```
<keep_running>1</keep_running>
```

VPN before logon is currently not supported in FortiClient v5.0 Patch Release 2 (Mac OS X).

VPN tunnel & script (Microsoft Windows)

Feature overview

This feature supports auto running a user-defined script after the configured VPN tunnel is connected or disconnected. The scripts are batch scripts in Windows and shell scripts in Mac OS X. They are defined as part of a VPN tunnel configuration on FortiGate's XML format Endpoint Profile. The profile will be pushed down to FortiClient from FortiGate. When FortiClient's VPN tunnel is connected or disconnected, the respective script defined under that tunnel will be executed.

Map a network drive after tunnel connection

The script will map a network drive and copy some files after the tunnel is connected.

```
<on_connect>
  <script>
    <os>windows</os>
      <script>
        <script>
          <![CDATA[
net use x: \\192.168.10.3\ftpshare /user:Honey Boo Boo
md c:\test
copy x:\PDF\*.* c:\test
              ]]>
        </script>
      </script>
  </on_connect>
```

Delete a network drive after tunnel is disconnected

The script will delete the network drive after the tunnel is disconnected.

```
<on_disconnect>
  <script>
    <os>windows</os>
    <script>
      <script>
        <![CDATA[
net use x: /DELETE
          ]]>
</script>
      </script>
    </script>
</on_disconnect>
```

VPN tunnel & script (Mac OS X)

Map a network drive after tunnel connection

The script will map a network drive and copy some files after the tunnel is connected.

```
<on_connect>
  <script>
    <os>mac</os>
    <script>
      /bin/mkdir /Volumes/installers
      /sbin/ping -c 4 192.168.1.147 >
           /Users/admin/Desktop/dropbox/p.txt
      /sbin/mount -t smbfs
           //kimberly:RigUpTown@ssldemo.fortinet.com/installer
```

```
            s /Volumes/installers/ >
            /Users/admin/Desktop/dropbox/m.txt
        /bin/mkdir /Users/admin/Desktop/dropbox/dir
        /bin/cp /Volumes/installers/*.log
            /Users/admin/Desktop/dropbox/dir/.
    </script>
  </script>
</on_connect>
```

Delete a network drive after tunnel is disconnected

The script will delete the network drive after the tunnel is disconnected.

```
<on_disconnect>
  <script>
    <os>mac</os>
    <script>
      /sbin/umount /Volumes/installers
      /bin/rm -fr /Users/admin/Desktop/dropbox/*
  </script>
  </script>
</on_disconnect>
```

For more information, see the *FortiClient v5.0 Patch Release 3 XML Reference* at the Fortinet Technical Documentation site, http://docs.fortinet.com.

Vulnerability Scan

Vulnerability Scan

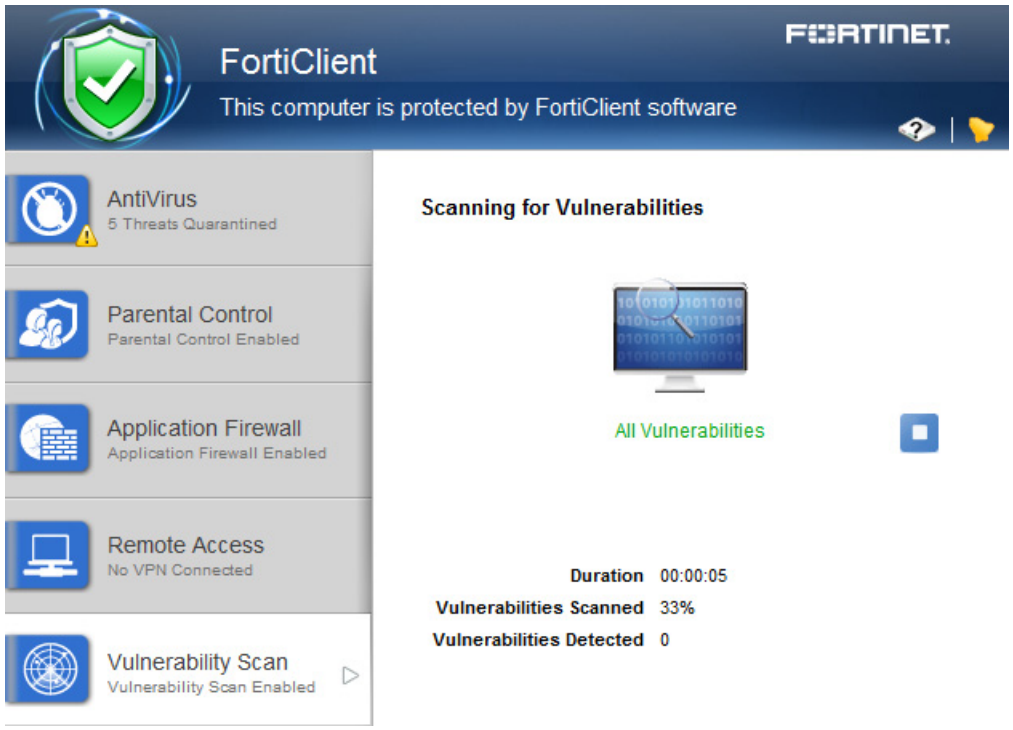
FortiClient v5.0 includes an *Vulnerability Scan* module to check your personal computer for known system vulnerabilities.

This section describes how to enable *Vulnerability Scan* and configuration options.

Scan Now

To perform a vulnerability scan, select the *Scan Now* button in the FortiClient console. FortiClient will scan your personal computer for known vulnerabilities. The console displays the date of the last scan above the button.

Figure 69: Vulnerability scan in progress



Update Now

Select the *Update Now* button in the FortiClient console to update the vulnerability signature.

You can select to use a FortiManager device for client software and signature updates. When configuring the endpoint profile, select *Use FortiManager for client software/signature updates* to enable the feature and enter the IP address of your FortiManager device.

View Vulnerabilities

When the scan is complete, FortiClient will display the number of vulnerabilities found in the FortiClient console. Select the *Found* link to view a list of vulnerabilities detected on your system.

Table 3: Vulnerabilities detected page

Vulnerabilities Detected in the Last 30 Days

Vulnerability Name	Severity	Details	Time
Most Recent Scan			
1 Adobe.Flash.Player.and.AIR.Multiple.Vulnerabilities.APSB12-24	Critical	33877	24/12/2012 2:35:21 PM
2 MS.VS.Active.Template.Library.Remote.Code.Execution	Critical	20531	24/12/2012 2:35:21 PM
3 Oracle.Java.SE.Critical.Patch.Update.October.2012	Critical	33716	24/12/2012 2:35:21 PM
4 Oracle.Java.SE.Critical.Patch.Update.Advisory.February.2012	Critical	32669	24/12/2012 2:35:21 PM
5 Oracle.Java.SE.Critical.Patch.Update.February.2011	Critical	27928	24/12/2012 2:35:21 PM
6 Oracle.Java.SE.Critical.Patch.Update.June.2011	Critical	30899	24/12/2012 2:35:21 PM
7 Oracle.Java.Runtime.True.Type.Font.IDEF.Opcode.Buffer.Ove...	Critical	31444	24/12/2012 2:35:21 PM
8 Oracle.Java.Runtime.Environment.Memory.Corruption.Vulnera...	Critical	33599	24/12/2012 2:35:21 PM
9 Oracle.Java.MixerSequence.Array.Index.Remote.Code.Execut...	Critical	30551	24/12/2012 2:35:21 PM
10 Oracle.Java.FileDialog.Show.Buffer.Overflow	Critical	28761	24/12/2012 2:35:21 PM
11 Oracle.Java.SE.Critical.Patch.Update.June.2012	Critical	32430	24/12/2012 2:35:21 PM
12 Microsoft.XML.Core.Services.Remote.Code.Execution.Vulner...	Critical	32958	24/12/2012 2:35:21 PM
13 MS.Windows.Unauthorized.Digital.Certificates.Spoofing.KB2...	Critical	32685	24/12/2012 2:35:21 PM
14 Apple.Safari.Multiple.Vulnerabilities.APPLE-SA-2012-11-01-2	Critical	33927	24/12/2012 2:35:21 PM
15 Adobe.Flash.Player.and.AIR.Multiple.Vulnerabilities.APSB12-14	Critical	32255	24/12/2012 2:35:21 PM
16 Adobe.Flash.Player.and.AIR.Multiple.Vulnerabilities.APSB12-19	Critical	33028	24/12/2012 2:35:21 PM
17 Adobe.Flash.Player.and.AIR.Multiple.Vulnerabilities.APSB12-22	Critical	33582	24/12/2012 2:35:21 PM

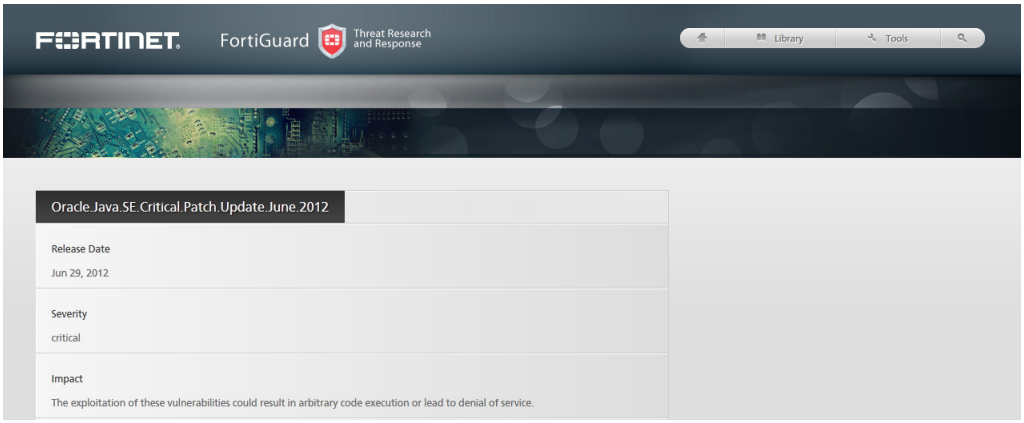
Close Clear

This page displays the following:

Vulnerability Name	The name of the vulnerability
Severity	The severity level assigned to the vulnerability; Critical, High, Medium, Low, Info.
Details	FortiClient vulnerability scan lists a Bugtraq (BID) number under the details column. You can select the BID to view details of the vulnerability on the FortiGuard site, or search the web using this BID number.
Time	The date and time that the vulnerability was detected.
Close	Close the window and return to the FortiClient console.
Clear	Clear the Vulnerability Scan results.

Select the *Details* ID number from the list to view information on the selected vulnerability on the FortiGuard site. The site details the release date, severity, impact, description, affected products, and recommended actions.

Figure 70: FortiGuard site details



Vulnerability Scan logging

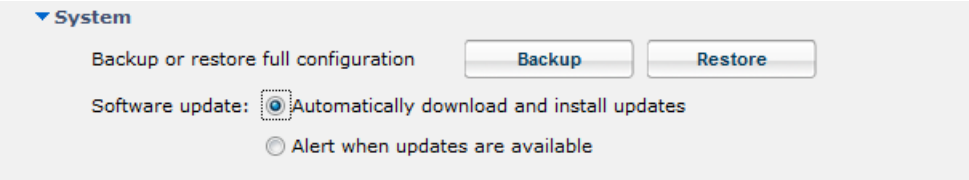
To configure Vulnerability Scan logging, select *File* in the toolbar, and select *Settings* in the drop-down menu. Select *Logging* to view the drop-down menu. Select *Vulnerability Scan* in the logging menu to enable logging for this module.

Settings

Backup or restore full configuration

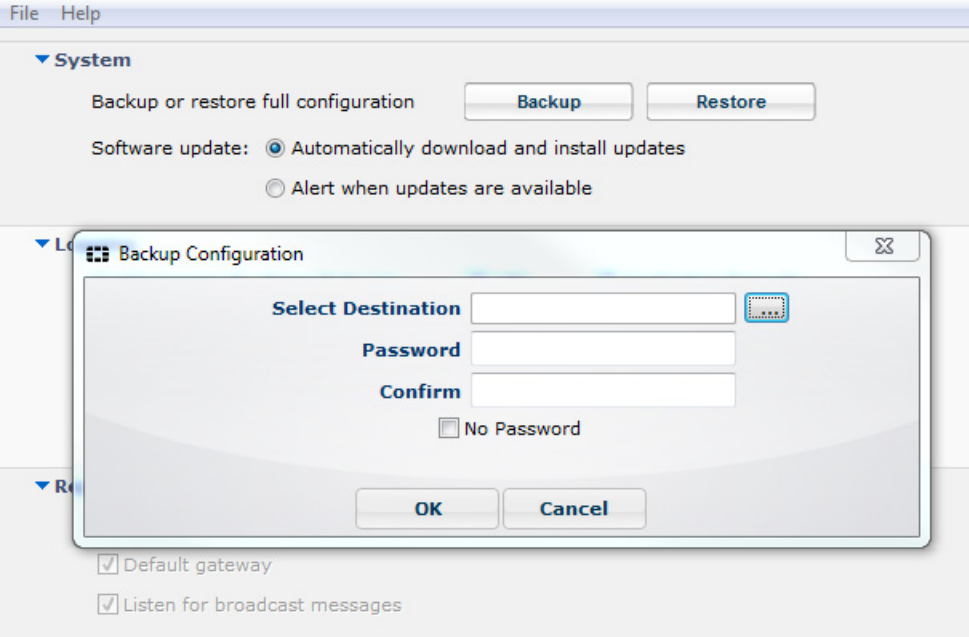
To backup or restore the full configuration file select *File* in the toolbar and select *Settings* in the drop-down menu. Select *System* to view the drop-down menu. In this menu you can perform a backup or restore a full configuration file.

Figure 71: Backup and restore options



When performing a backup you can select the file destination and save the file in an unencrypted or encrypted format.

Figure 72: Backup configuration dialog box



Logging

To configure logging, select *File* in the toolbar and select *Settings* in the drop-down menu. Select *Logging* to view the drop-down menu. In this menu you can configure logging for the following features:

- VPN
- Antivirus
- Update
- Application Firewall
- Parental Control
- Vulnerability Scan

You can specify the logging level and select to export logs or clear logs.

Figure 73: Logging options

The following table lists the logging levels and description:

Table 4: FortiClient logging levels

Logging Level	Description
Emergency	The system becomes unstable.
Alert	Immediate action is required.
Critical	Functionality is affected.
Error	An error condition exists and functionality could be affected.
Warning	Functionality could be affected.
Notice	Information about normal events.
Information	General information about system operations.
Debug	Debug FortiClient.

FortiClient can be configured via the endpoint profile to send traffic, vulnerability scan, and event logs to your FortiAnalyzer or FortiManager device running v5.0 Patch Release 2 or later.

Configure logging to FortiAnalyzer or FortiManager

To configure FortiClient to log to your FortiAnalyzer or FortiManager you require the following:

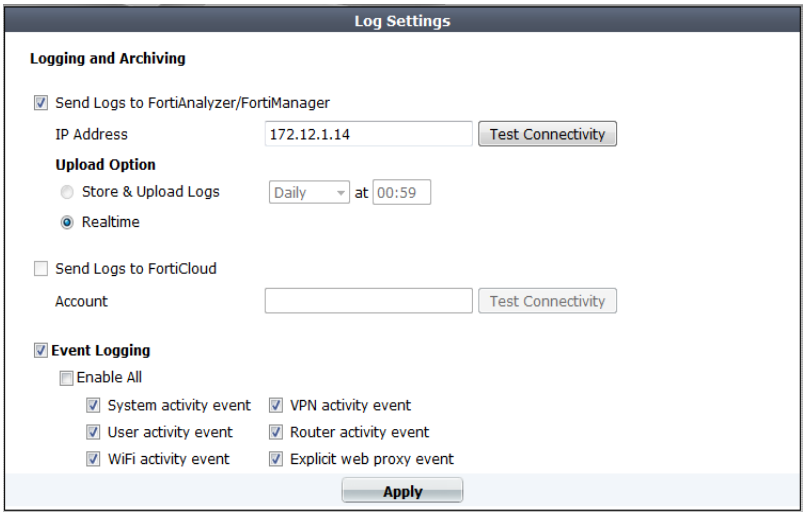
- FortiClient v5.0 Patch Release 2 or later
- A FortiGate device running FortiOS v5.0 Patch Release 2 or later
- A FortiAnalyzer or FortiManager device running v5.0 Patch Release 2 or later

The registered FortiClient device will send traffic logs, vulnerability scan logs, and event logs to the log device on port 514 TCP.

Enable logging on the FortiGate device:

1. On your FortiGate device, select *Log & Report* > *Log Config* > *Log Settings*.
2. The *Log Settings* window opens.

Figure 74: Log settings window



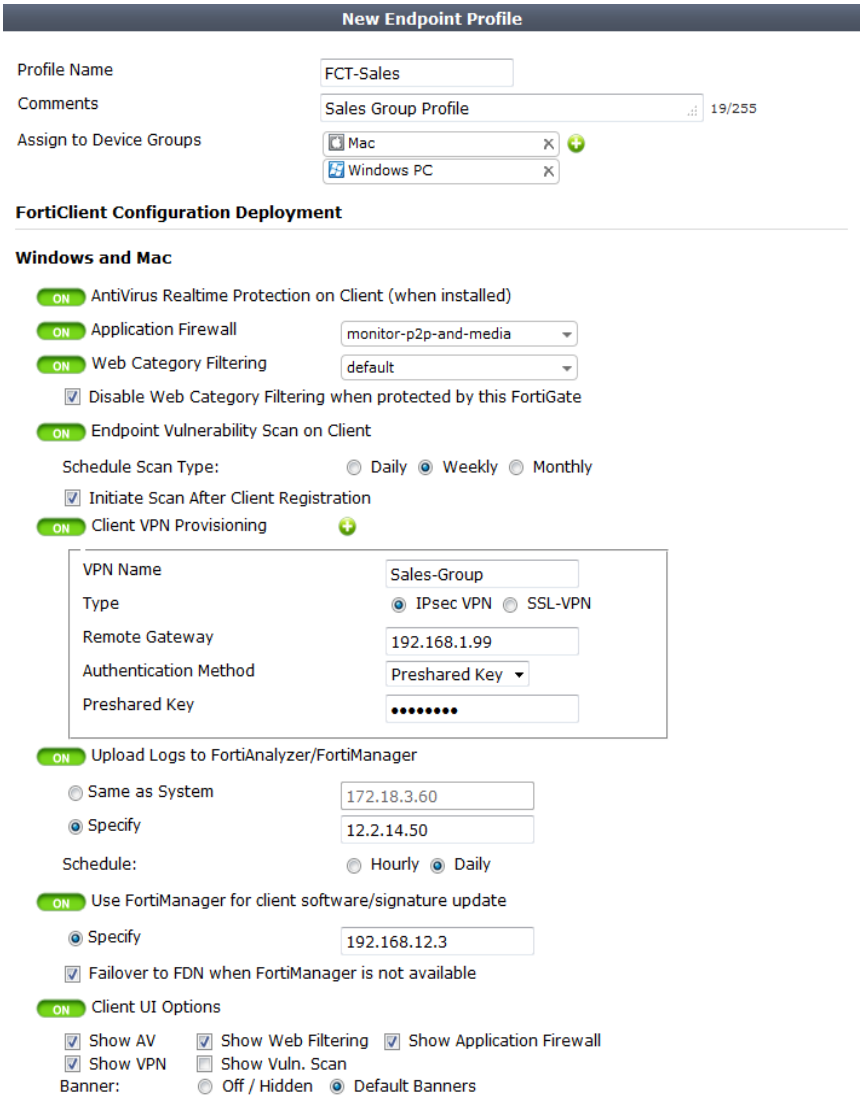
3. Select the *Send Logs to FortiAnalyzer/FortiManager* checkbox to enable this feature. Enter the IP address of your log device. You can select *Test Connectivity* to ensure your FortiGate is able to communicate with the log device on this IP address.
4. Select *Apply* to save the setting.

FortiClient must be able to access the FortiAnalyzer IP address in order to forward logs.

5. Select *User & Device* > *Device* > *Endpoint Profile*.

   The *Edit Profile* window opens.

Figure 75: Edit endpoint profile window



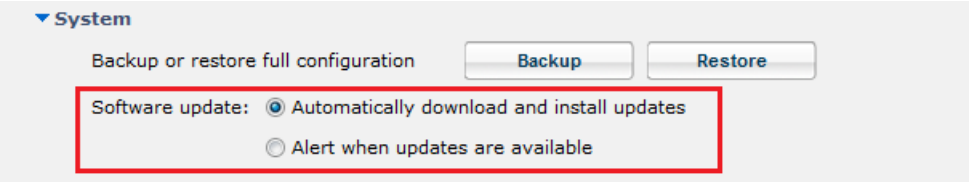
6. Under *FortiClient Configuration Deployment Windows and Mac*, toggle the *Upload Logs to FortiAnalyzer/FortiManager* feature to *ON*. You can select either *Same as System* which will follow the FortiGate settings or *Specify* to enter a different IP address. Under *Schedule*, select to upload logs *Hourly* or *Daily*. Selecting *Change* beside the IP address text box will re-direct you to the Log settings window.
7. Select *Apply* to save the setting. Once the endpoint profile change is synchronized with the client, you will start receiving logs from registered clients on your FortiAnalyzer/FortiManager system.

To download the FortiClient log files on the FortiAnalyzer go to the *Log View* tab, select the ADOM, and select the *FortiClient* menu object.

Updates

To configure updates, select *File* in the toolbar and select *Settings* in the drop-down menu. Select *System* to view the drop-down menu. In this menu you can configure the behavior of FortiClient when a new software version is available on the FortiGuard Distribution Servers (FDS).

Figure 76: Update options



You can select to use a FortiManager device for client software and signature updates. When configuring the endpoint profile, select *Use FortiManager for client software/signature updates* to enable the feature and enter the IP address of your FortiManager device.

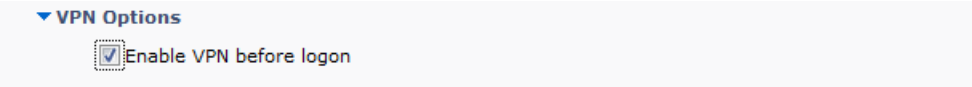
To configure FortiClient to use FortiManager for software and signature updates:

1. Select *User & Device* > *Device* > *Endpoint Profile*.
2. Toggle the *Use FortiManager for client software/signature update* option to *ON*.
3. You can select either *Same as System* which will follow the FortiGate settings or *Specify* to enter a different IP address.
4. Select the checkbox beside *Failover to FDN when FortiManager is not available* to have FortiClient receive updates from the FortiGuard Distribution Network when the FortiManager is not available to ensure your clients are always protected.
5. Select *Apply* to save the setting.

VPN options

To configure VPN options, select *File* in the toolbar and select *Settings* in the drop-down menu. Select *VPN Options* to view the drop-down menu. In this menu you can configure to enable VPN before logon.

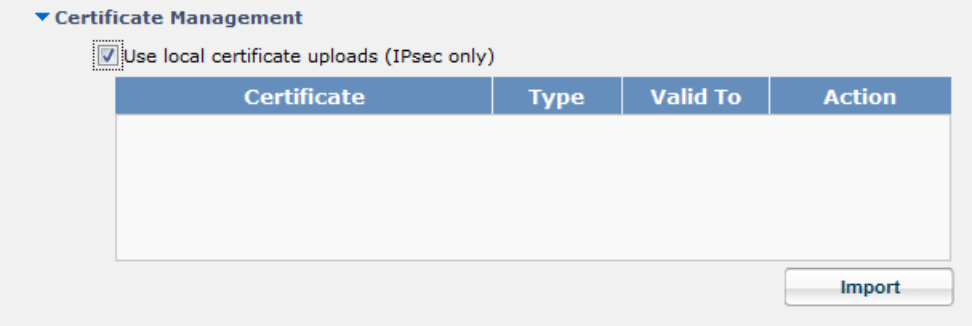
Figure 77:VPN options



Certificate Management

To configure VPN certificates, select *File* in the toolbar and select *Settings* in the drop-down menu. Select *Certificate Management* to view the drop-down menu. In this menu you can configure IPsec VPN to use local certificates and import certificates to FortiClient.

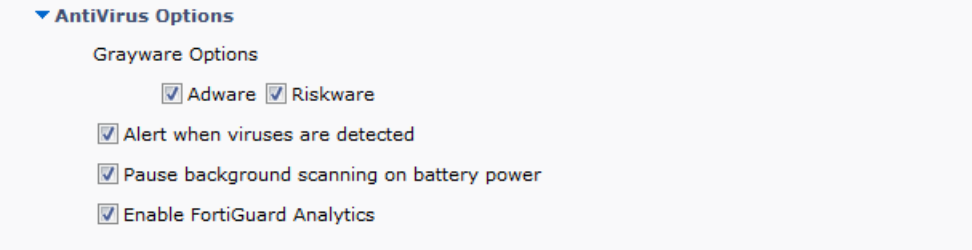
Figure 78: Certificate management options



Antivirus options

To configure antivirus options, select *File* in the toolbar and select *Settings* in the drop-down menu. Select *AntiVirus Options* to view the drop-down menu. In this menu you can configure grayware options and the behavior of FortiClient when a virus is detected.

Figure 79: Antivirus options



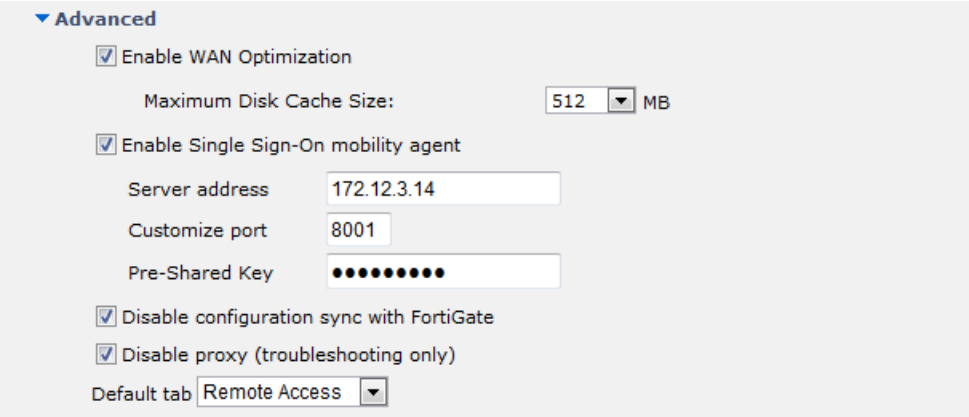
Configure the following settings:

Grayware Options	Grayware is an umbrella term applied to a wide range of malicious applications such as spyware, adware and key loggers that are often secretly installed on a user's computer to track and/or report certain information back to an external source without the user's permission or knowledge.
Adware	Select to enable adware detection and quarantine during the antivirus scan.
Riskware	Select to enable riskware detection and quarantine during the antivirus scan.
Alert when viruses are detected	Select to display notification message window when a virus is detected.
Pause background scanning on battery power	Select to pause background scanning when on battery power.
Enable FortiGuard Analytics	Select to automatically send suspicious files to the FortiGuard Network for analysis.

Advanced options

To configure advanced options, select *File* in the toolbar, and select *Settings* in the drop-down menu. Select *Advanced* to view the drop-down menu. In this menu you can configure WAN Optimization, Single Sign-On, configuration sync with FortiGate, disable proxy, and the default tab when FortiClient is started.

Figure 80: Advanced options



Configure the following settings:

Advanced	Advanced FortiClient settings.
Enable WAN Optimization	Select to enable WAN Optimization. You should enable only if you have a FortiGate device and your FortiGate is configured for WAN Optimization.
Maximum Disk Cache Size	Select to configure the maximum disk cache size. The default value is 512MB.
Enable Single Sign-On mobility agent	Select to enable Single Sign-On Mobility Agent for FortiAuthenticator. To use this feature you need to apply a FortiClient SSO mobility agent license to your FortiAuthenticator device.
Server address	Enter the FortiAuthenticator IP address.
Customize port	Enter the port number. The default port is 8001.
Pre-Shared Key	Enter the pre-shared key. The pre-shared key should match the key configured on your FortiAuthenticator device.
Disable configuration sync with FortiGate	Select to disable configuration synchronization with FortiGate.
Disable proxy (troubleshooting only)	Select to disable proxy when troubleshooting FortiClient.
Default tab	Select the default tab to be displayed when opening FortiClient.

Single Sign-On Mobility Agent

The FortiClient Single Sign-On Mobility Agent acts as a client that updates with FortiAuthenticator with user logon and network information.

FortiClient/FortiAuthenticator Protocol

The FortiAuthenticator listens on a configurable TCP port. FortiClient connects to FortiAuthenticator using TLS/SSL with two-way certificate authentication. The FortiClient sends a logon packet to FortiAuthenticator, which replies with an acknowledgement packet.

FortiClient/FortiAuthenticator communication requires the following:

- The IP address should be unique in the entire network.
- The FortiAuthenticator should be accessible from clients in all locations.
- The FortiAuthenticator should be accessible by all FortiGates.

FortiClient Single Sign-On Mobility Agent requires a FortiAuthenticator running v2.0.0 GA build 0006 or later. Enter the FortiAuthenticator (server) IP address, port number, and the pre-shared key configured on the FortiAuthenticator.

Enable Single Sign-On Mobility Agent on FortiClient:

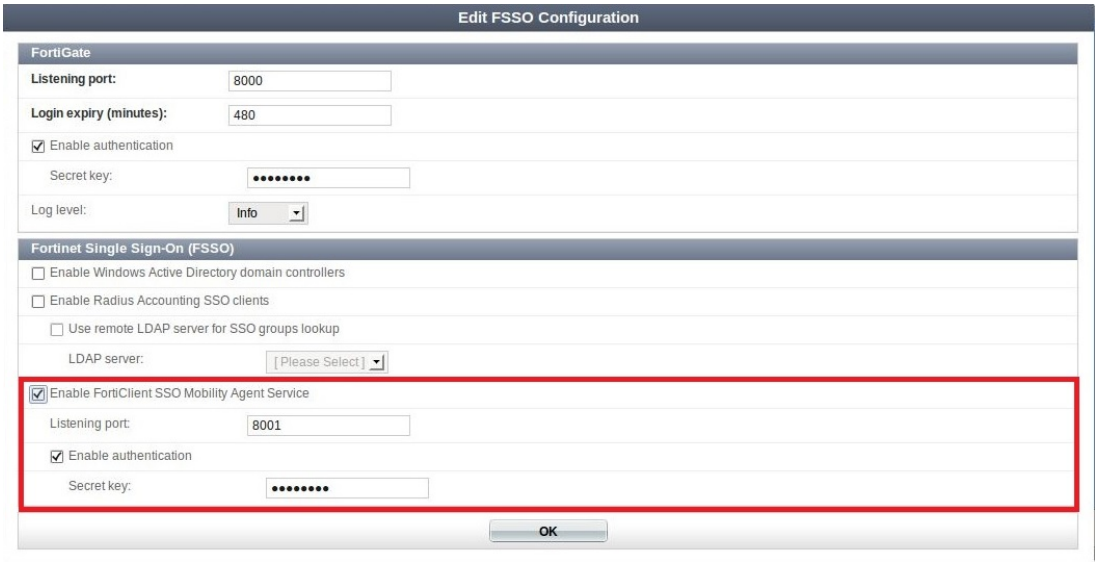
1. Select *File* in the toolbar and select *Settings* in the drop-down menu.
2. Select *Advanced* to view the drop-down menu.
3. Select to *Enable Single Sign-On mobility agent*.
4. Enter the FortiAuthenticator server address and the pre-shared key.

Enable FortiClient SSO Mobility Agent Service on the FortiAuthenticator:

1. Select *SSO & Dynamic Policies* > *SSO* > *Options*.

   The *Edit FSSO Configuration* page opens.

Figure 81: FortiAuthenticator configuration window



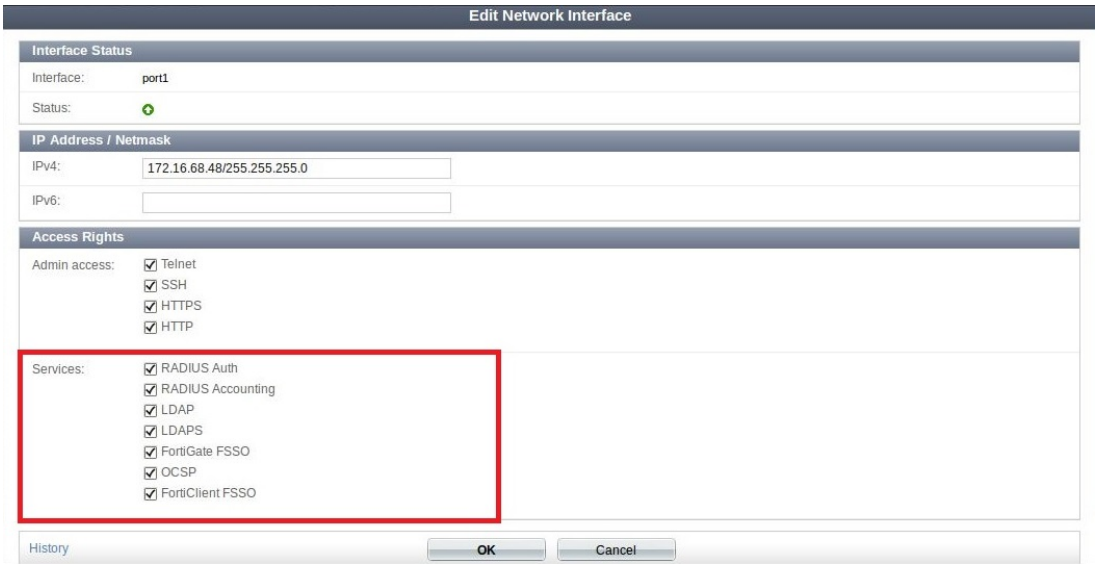
2. Select *Enable FortiClient SSO Mobility Agent Service* and a TCP port value for the listening port.
3. Select *Enable authentication* and enter a secret-key value.
4. Select *OK* to save the setting.

To enable FortiClient FSSO services on the interface:

1. Select *System* > *Network* > *Interface*.

   The *Edit Network Interface* window opens.

Figure 82: Edit network interface window



2. Select *Edit* to edit the network interface, select *FortiClient FSSO* to enable.

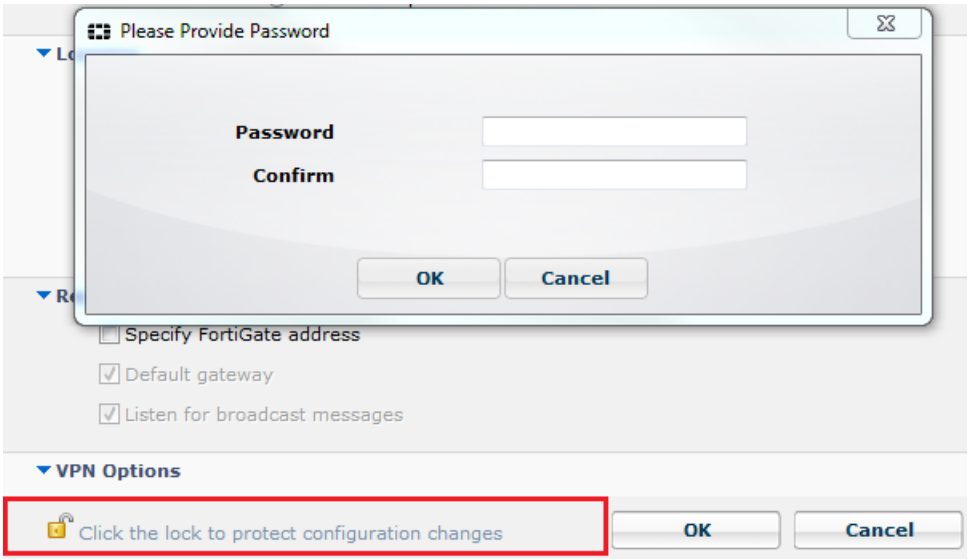
3. Select *OK* to save the setting.

To enable the FortiClient SSO Mobility Agent Service on the FortiAuthenticator, you must first apply the applicable FortiClient license for FortiAuthenticator. For more information, see the *FortiAuthenticator v2.0 Administration Guide* at http://docs.fortinet.com. For information on purchasing a FortiClient license for FortiAuthenticator, please contact your authorized Fortinet reseller.

Configuration lock

To prevent unauthorized changes to the FortiClient configuration, select the lock icon located at the bottom left of the *Settings* page. You will be prompted to enter and confirm a password. When the configuration is locked, configuration changes are restricted and FortiClient cannot be shut down or uninstalled.

Figure 83: Configuration lock window and dialog box



When the configuration is locked you can perform the following actions:

- Antivirus
  - Complete an antivirus scan, view threats found, and view logs
  - Select *Update Now* to update signatures
- Parental Control
  - View violations
- Application Firewall
  - View applications blocked
- Remote Access
  - Configure, edit, or delete an IPsec VPN or SSL VPN connection
  - Connect to a VPN connection
- Vulnerability Scan
  - Complete a vulnerability scan of the system
  - View vulnerabilities found
- Register and unregister FortiClient for Endpoint Control

- Settings
  - Export FortiClient logs
  - Backup the FortiClient configuration

To perform configuration changes or to shut down FortiClient, select the lock icon and enter the password used to lock the configuration.

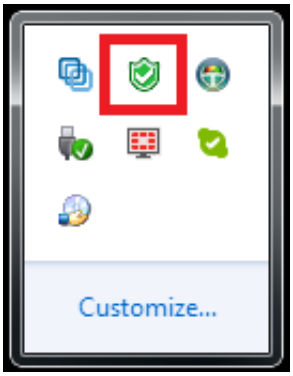
FortiTray

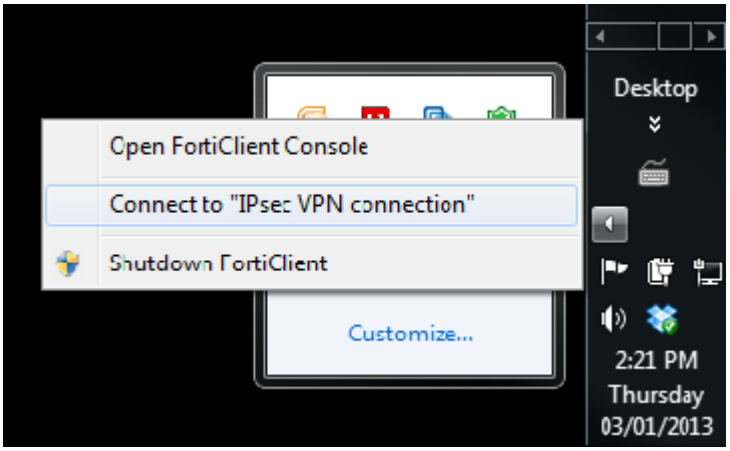
When FortiClient is running on your system, you can select the FortiTray icon in the Windows system tray to perform various actions. The FortiTray icon is available in the system tray even when the FortiClient console is closed.

- Default menu options
  - Open FortiClient console
  - Shutdown FortiClient
- Dynamic menu options depending on configuration
  - Connect to a configured IPsec VPN or SSL VPN connection
  - Display the antivirus scan window (if a scheduled scan is currently running)
  - Display the Vulnerability scan window (if a vulnerability scan is running)

If you hover the mouse cursor over the FortiTray icon, you will receive various notifications including the version, antivirus signature, and antivirus engine.

Figure 84: System tray icon and FortiTray menu



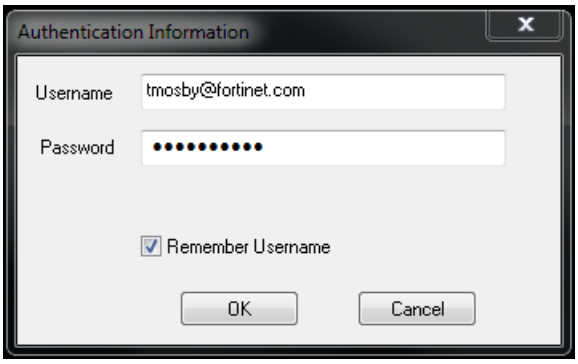


When the configuration is locked, the option to shut down FortiClient from FortiTray is greyed out.

Connect to a VPN connection

To connect to a VPN connection from FortiTray, select the Windows System Tray and right-click in the FortiTray icon. Select the connection you wish to connect to, enter your username and password in the authentication window, and select *OK* to connect.

Figure 85: Authentication window



Index